Citrix Access Gateway Standard Edition Administratorhandbuch

Citrix Access Gateway™ 4.5

Hinweise zu Copyright und Marken

Die Verwendung des in diesem Handbuch beschriebenen Produkts unterliegt der Annahme der Endbenutzerlizenzvereinbarung. Eine druckbare Kopie der Endbenutzerlizenzvereinbarung finden Sie auf der Produkt-CD-ROM.

Die in diesen Unterlagen enthaltenen Angaben und Daten können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Firmen, sonstigen Namen und Daten sind frei erfunden, sofern nichts anderes angegeben ist. Ohne ausdrückliche schriftliche Erlaubnis von Citrix Systems, Inc. darf kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, weder elektronisch noch mechanisch.

© 2005 - 2006 Citrix Systems, Inc. Alle Rechte vorbehalten.

Citrix, ICA (Independent Computing Architecture) und Program Neighborhood sind eingetragene Marken und Citrix Presentation Server, Citrix Access Gateway und SpeedScreen sind Marken von Citrix Systems, Inc. in den USA und anderen Ländern.

RSA © 1996-1997 RSA Security Inc. Alle Rechte vorbehalten.

Dieses Produkt enthält Software, die von OpenSSL Project für die Verwendung mit dem OpenSSL Toolkit (http://www.openssl.org) entwickelt wurde.

AOL Instant Messenger ist eine eingetragene Marke von America Online, Inc.

McAfee Personal Firewall Plus ist eine eingetragene Marke von McAfee, Inc.

Symantec und das Symantec-Logo sind, in den USA und bestimmten anderen Ländern, Marken oder eingetragene Marken der Symantec Corporation.

ZoneAlarm ist eine Marke oder eingetragene Marke von Zone Labs LLC in den USA und anderen Ländern.

Win32-Client: Teile dieser Software basieren auf Code der O'Reilly Media, Inc. 1998. (CJKV Information Processing, von Ken Lunde. ISBN: 1565922247.) Alle Rechte vorbehalten.

Lizenzierung: Teile dieser Dokumentation über Globetrotter, Macrovision und FLEXlm sind urheberrechtlich geschützt von © 2005 Macrovision Corporation. Alle Rechte vorbehalten.

Anerkennung von Marken

Adobe, Acrobat und PostScript sind Marken oder eingetragene Marken von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Apple, LaserWriter, Mac, Macintosh, Mac OS und Power Mac sind eingetragene Marken oder Marken von Apple Computer Inc.

SafeWord Remote Access, SafeWord for Citrix und SafeWord PremierAccess sind eingetragene Marken oder Marken der Secure Computing Corporation.

Java, Sun und SunOS sind Marken oder eingetragene Marken von Sun Microsystems, Inc. in den USA und anderen Ländern. Solaris ist eine eingetragene Marke von Sun Microsystems, Inc., die dieses Produkt nicht getestet oder anerkannt haben.

Microsoft, MS-DOS, Windows, Windows Media, Windows Server, Windows NT, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003, Win32, Outlook, ActiveX, Active Directory, MSN Messenger und DirectShow sind entweder eingetragene Marken oder Marken von Microsoft Corporation in den USA und/oder anderen Ländern.

Firefox ist eine Marke der Mozilla Foundation.

BlackICE PC Protection ist eine Marke der Network Ice Corporation.

ICQ ist eine Marke oder Dienstleistungsmarke von ICQ.

UNIX ist eine eingetragene Marke von The Open Group.

Softerra ist eine Marke von Softerra LLC.

Lizenzierung: Globetrotter, Macrovision und FLEXlm sind Marken und/oder eingetragene Marken der Macrovision Corporation.

Alle anderen Marken und eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber.

Dokumentcode: 27. November 2006, 14:35 (KM)

Inhalt

Kapitel 1 Einführung

Hinweise zur Benutzung dieses Handbuchs. 13
Typografische Konventionen 14
Service und technischer Support 15
Subscription Advantage 15
Knowledge Center-Watches 16
Schulung und Zertifizierung 16
Literaturhinweise 16

Kapitel 2 Einführung in das Citrix Access Gateway

Access Gateway-Technologien 18
Access Gateway-Betriebsmodi. 18
Funktionen des Access Gateways 19
Neue Funktionen. 20

Kapitel 3 Planen der Bereitstellung

Bereitstellen des Access Gateways. 23
Access Gateway in der DMZ des Netzwerks. 24
Installieren des Access Gateways in der DMZ. 25
Access Gateway-Konnektivität in der DMZ 25
Access Gateway in einem sicheren Netzwerk 26
Access Gateway-Konnektivität in einem sicheren Netzwerk 26
Überlegungen zur Sicherheit 27
Konfigurieren der sicheren Zertifikatverwaltung 27
Unterstützung bei der Authentifizierung. 28
Bereitstellen des Gateways mit Citrix Presentation Server 28
Bereitstellen des Gateways in der DMZ mit Citrix Presentation Server 29
Bereitstellen des Access Gateways in einer Double-Hop-DMZ 33
Bereitstellen weiterer Geräte für Lastausgleich und Failover 35
Bereitstellen von Access Gateway-Geräten hinter einem Load Balancer 36

Bereitstellen von Access Gateway Advanced Edition 37
Mehrere Server in einer Access-Serverfarm 38

Kapitel 4 Erstmalige Installation des Access Gateways

Vorbereitung der Installation des Access Gateways 39
Für die Installation erforderliches Zubehör und Informationen 39
Einrichten der Access Gateway-Hardware 41
Konfigurieren der TCP/IP-Einstellungen für das Access Gateway 42
Konfigurieren der TCP/IP-Einstellungen mit dem seriellen Kabel 42
Konfigurieren der TCP/IP-Einstellungen mit Netzwerkkabeln 45
Konfigurieren der TCP/IP-Einstellungen für eine Double-Hop-Bereitstellung 48
Neustarten des Access Gateways 48

Kapitel 5 Konfigurieren des Access Gateways für die Netzwerkumgebung

Installieren von Lizenzen 49
Abrufen der Lizenzdateien 50
Konfigurieren von Lizenzen für mehrere Geräte 52
Informationen zu Lizenzen 53
Aktualisieren vorhandener Lizenzen 54
Kulanzzeitraum für die Lizenzierung 54
Testen der Lizenzinstallation 54
Erstellen und Installieren von Zertifikaten 55
Übersicht über Zertifikatsignieranforderungen 56
Erstellen einer Zertifikatsignieranforderung 57
Installieren eines Zertifikats und eines privaten Schlüssels von einem Windows-Computer aus 60
Installieren von Stammzertifikaten auf dem Access Gateway 60
Installieren mehrerer Stammzertifikate 61
Konfigurieren weiterer Netzwerkeinstellungen 62
Konfigurieren von Namensdienstanbietern 62
Bearbeiten der HOSTS-Datei 63
Konfigurieren von dynamischen und statischen Routen 64
Konfigurieren von Datum und Uhrzeit auf dem Access Gateway 70
Konfigurieren eines NTP-Servers 70
Verwenden der Standardportalseite 71
Installieren des Secure Access Client für Linux 74
Konfigurieren des Netzwerkzugriffs 74

Kapitel 6 Konfigurieren der Authentifizierung und Autorisierung

Voraussetzungen zum Konfigurieren der Authentifizierung auf dem Access Gateway 78
Konfigurieren der Authentifizierung auf dem Access Gateway 78
Konfigurieren des Bereichs „Default“ 80
Erstellen von zusätzlichen Bereichen 82
Konfigurieren der lokalen Authentifizierung 83
Konfigurieren lokaler Benutzer 84
Zuweisen von Benutzern zu mehreren Gruppen 85
Ändern von Kennwörtern für Benutzer 85
Konfigurieren von LDAP-Authentifizierung und -Autorisierung 86
Konfigurieren der LDAP-Autorisierung 90
Gruppenattributfelder für die LDAP-Autorisierung 92
Verwenden von Zertifikaten für sichere LDAP-Verbindungen 93
Bestimmen der Attribute in Ihrem LDAP-Verzeichnis 94
Konfigurieren von RADIUS-Authentifizierung und -Autorisierung 95
RADIUS-Autorisierung 98
Auswählen der RADIUS-Authentifizierungsprotokolle 99
Konfigurieren der RSA SecurID-Authentifizierung 100
Konfigurieren der RSA-Einstellungen für einen Cluster 103
Zurücksetzen des Node Secret 103
Konfigurieren der Authentifizierung mit Secure Computing SafeWord 104
Konfigurieren der SafeWord-Einstellungen auf dem Access Gateway 105
Konfigurieren der Autorisierung mit SafeWord 106
Konfigurieren von NTLM-Authentifizierung und -Autorisierung 107
Konfigurieren der NTLM-Autorisierung 109
Konfigurieren von Zweimethodenauthentifizierung 110
Ändern der Beschriftung von Kennwortfeldern 111

Kapitel 7 Konfigurieren von Netzwerkzugriff und Gruppenressourcen

Konfigurieren des Netzwerkrouting 114
Bereitstellen von Netzwerkzugriff für Benutzer 114
Aktivieren von Split-Tunneling und zugänglichen Netzwerken 116
Konfigurieren von Benutzergruppen 117
Konfigurieren von Zugriffssteuerungslisten 118
Erstellen lokaler Benutzergruppen 119
Konfigurieren von Ressourcengruppen 119
Erstellen von Benutzergruppen 121
Eigenschaften der Standardgruppe („Default“) 122

Konfigurieren von Ressourcen für eine Benutzergruppe. 123
Konfigurieren von Benutzern, die mehreren Gruppen angehören 124
Konfigurieren von Netzwerkressourcen. 125
Zulassen und Verweigern von Netzwerkressourcen und Anwendungsrichtlinien 127
Festlegen von Anwendungsrichtlinien 129
Konfigurieren von Endpunktrichtlinien und -ressourcen. 131
Konfigurieren von Endpunktressourcen 131
Erstellen einer Endpunktrichtlinie für eine Gruppe 133
Festlegen der Priorität von Gruppen. 135
Konfigurieren von Richtlinien zur Überprüfung vor der Authentifizierung . .137

Kapitel 8 Konfigurieren von Benutzerverbindungen für den Secure Access Client

Systemvoraussetzungen 140
Betriebssysteme. 140
Webbrowser. 141
Funktionsweise von Benutzerverbindungen 141
Einrichten des sicheren Tunnels 142
Tunneln des privaten Netzwerkverkehrs über sichere Verbindungen 142
Beenden des sicheren Tunnels und Zurücksenden von Paketen an den Client 145
Unterstützung für den Secure Access Client 146
Konfigurieren von Proxyservern für den Secure Access Client 148
Konfigurieren des Secure Access Clients für Benutzer ohne Administratorrechte. 149
Konfigurieren von Single Sign-on für Windows-Betriebssysteme 149
Herstellen von Verbindungen mit früheren Versionen des Secure Access Clients 150
Herstellen einer Verbindung mit einer Webadresse. 152
Installieren von ActiveX Helper 152
Anmelden mit dem Secure Access Client. 153
Verbindungen im Kioskmodus. 157
Erstellen einer Kioskmodusressource 160
Konfigurieren von Clientanwendungen für den Kioskmodus 161
Konfigurieren von Dateifreigaben für den Kioskmodus 165
Konfigurieren der Authentizierungsanforderungen nach einer Netzwerkunterbrechung 167

Konfigurieren weiterer Gruppeneigenschaften 168
Aktivieren von IP-Pooling. 168
Aktivieren von Split DNS 169
Aktivieren von internem Failover 170
Aktivieren von Domänenanmeldeskripten 170
Aktivieren von Secure Access Client-Sitzungstimeouts 171
Konfigurieren von Websitzungstimeouts 172
Deaktivieren von Desktopfreigaben 173
Schließen und Deaktivieren von Benutzerverbindungen. 173
Verarbeitung von Verbindungen im Access Gateway 174
Schließen einer Verbindung zu einer Ressource 175
Deaktivieren und Aktivieren eines Benutzers 175
Anfordern von Clientzertifikaten für die Authentifizierung 176
Definieren von Clientzertifikatskriterien 177
Verwenden von Clientzertifikaten mit Access Gateway Advanced Edition . .178
Installieren von Stammzertifikaten. 179
Abrufen eines Stammzertifikats von einer Zertifizierungsstelle 179
Installieren von Stammzertifikaten auf einem Clientgerät. 179
Auswählen einer Verschlüsselungsart für Clientverbindungen. 180
Unterstützung von VoIP-Softphones 181
Verbessern von VoIP-Verbindungen 182

Kapitel 9 Konfigurieren der Anmelde- und Portalseiten für den Secure Access Client

Konfigurieren der Access Gateway-Anmeldeseiten 183
Aktivieren der Anmeldeseitenauthentifizierung. 183
Anpassen der Anmeldeseite 184
Access Gateway-Portalseitenvorlagen 185
Herunterladen von und Arbeiten mit Portalseitenvorlagen 186
Verwenden des ActiveX-Steuerelements 188
Installieren benutzerdefinierter Portalseitendateien 188
Einfügen von Links zu Clients auf Ihrer Website. 189
Auswählen einer Portalseite für eine Gruppe 190
Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen 190
Anmelden mit Zweimethodenauthentifizierung 191
Anmelden, wenn Vorauthentifizierungsrichtlinien konfiguriert sind 192

Kapitel 10 Bereitstellen von Zugriff auf veröffentlichte Anwendungen

Benutzerverbindungen zu einer Serverfarm. 194
Ersetzen von Secure Gateway 197
Vorbereiten der Migration auf das Access Gateway 200
Migrieren von Secure Gateway auf das Access Gateway 201
Überwachen des Access Gateways nach der Installation. 204
Konfigurieren des Webinterface. 204
Bereitstellen des Webinterface parallel zum Access Gateway in der DMZ . .205
Bereitstellen des Webinterface hinter dem Access Gateway in der DMZ. . . .206
Bereitstellen des Webinterface im sicheren Netzwerk. 207
Konfigurieren des Webinterface für die Authentifizierung. 207
Einrichten und Testen des Webinterface 209
Konfigurieren des Webinterface. 209
Konfigurieren der Secure Ticket Authority 212
Konfigurieren der ICA-Zugriffssteuerung. 214
Verwenden des Webinterface als Anmeldeseite 216
Konfigurieren von Single Sign-On beim Webinterface. 216
Konfigurieren des Access Gateways für Single Sign-On beim Webinterface 218
Konfigurieren des Webinterface für Single Sign-On. 219
Aktivieren der Sitzungszuverlässigkeit 222

Kapitel 11 Bereitstellen des Access Gateways in einer Double-Hop-DMZ

Datenübertragung in einer Double-Hop-DMZ-Konfiguration 225
Clientauthentifizierung 226
Erstellung von Sitzungstickets 227
Verbindungsherstellung. 227
Vorbereiten der Bereitstellung einer Double-Hop-DMZ. 228
Unterstützen von Lastausgleich 229
Verwenden der Anmeldeseitenauthentifizierung in einer Double-Hop-DMZ 230
Planen der Installation des Access Gateway Administration Tools. 232
Öffnen von Ports und Verwalten von Zertifikaten. 234
Für die Bereitstellung erforderliche Komponenten 234

Installieren des Access Gateways in einer Double-Hop-DMZ 235
Schritt 1: Installieren eines Access Gateways in der ersten DMZ 236
Schritt 2: Aktivieren oder Deaktivieren der Anmeldeseitenauthentifizierung.236
Schritt 3: Konfigurieren des Access Gateways zur Weiterleitung von Verbindungen an das Webinterface 237
Schritt 4: Installieren eines Access Gateways in der zweiten DMZ 238
Schritt 5: Konfigurieren des Access Gateways für die Kommunikation mit dem Access Gateway-Proxy 239
Schritt 6: Konfigurieren des Access Gateway-Proxys für die Kommunikation mit dem Access Gateway 241
Schritt 7: Konfigurieren des Access Gateways für den Secure Ticket Authority- und ICA-Datenverkehr 242
Schritt 8: Öffnen der entsprechenden Ports in den Firewalls 244
Schritt 9: Verwalten von SSL-Zertifikaten in einer Double-Hop-DMZ-Bereitstellung 246
Herstellen einer Clientverbindung in einer Double-Hop-DMZ. 250
Clientauthentifizierung 250
Erstellung von Sitzungstickets 251
Starten des Clients 252
Verbindungsherstellung. 252

Kapitel 12 Warten des Access Gateways

Access Gateway-Verwaltungstools 256
Administration Tool 256
Administration Portal 257
Überwachen des Access Gateways mit dem Administration Desktop 260
Aktualisieren der Access Gateway-Software 261
Installieren des Software-Upgrades 262
Neuinstallieren der Access Gateway-Software 263
Speichern und Wiederherstellen der Access Gateway-Konfiguration 264
Neustarten und Herunterfahren des Access Gateways 265
Neustarten des Access Gateways 265
Herunterfahren des Access Gateways. 266
Initialisieren des Access Gateways. 266
Zulassen von ICMP-Verkehr 267

Konfigurieren persönlicher Firewalls von Drittanbietern 267
BlackICE PC Protection 268
McAfee Personal Firewall Plus. 268
Norton Personal Firewall. 269
Sygate Personal Firewall (kostenlose und Pro-Version) 269
Tiny Personal Firewall 269
ZoneAlarm Pro 270

Kapitel 13 Installieren zusätzlicher Access Gateway-Geräte

Erstellen eines Clusters mit Access Gateway-Geräten 273
Konfigurieren mehrerer Geräte für die Verwendung eines Load Balancers. 275
Konfigurieren des Lastausgleichs 276
Konfigurieren von Access Gateway-Geräten für den Betrieb hinter einem Load Balancer 277
Konfigurieren von Access Gateway-Failover 280

Anhang A Überwachen des Access Gateways

Anzeigen und Herunterladen von Systemmeldungsprotokollen 283
Anzeigen von Secure Access Client-Verbindungsprotokollen 285
Weiterleiten von Systemmeldungen an einen Systemprotokollserver. 286
Aktivieren und Anzeigen von SNMP-Protokollen 286
Beispiel für eine MRTG-Ausgabe 287
Anzeigen von Systemstatistiken. 288
Überwachen der Access Gateway-Operationen. 288

Anhang B Sichern von Verbindungen mit digitalen Zertifikaten

Einführung in Sicherheitsprotokolle, Kryptografie und digitale Zertifikate 291
Einführung in Sicherheitsprotokolle 291
Einführung in die Kryptografie. 292
Digitale Zertifikate und Zertifizierungsstellen 295
Beantragen von Zertifikaten 299
Ihr Unternehmen hat eine eigene Zertifizierungsstelle. 299
Ihr Unternehmen hat keine eigene Zertifizierungsstelle. 299
Beantragen von Serverzertifikaten 300
Digitale Zertifikate und deren Verwendung im Access Gateway 300

Verwenden von Windows-Zertifikaten 301
Entschlüsseln des privaten Schlüssels. 302
Umwandeln in ein PEM-formatiertes Zertifikat. 302
Kombinieren des privaten Schlüssels mit dem signierten Zertifikat 304
Generieren vertrauenswürdiger Zertifikate für mehrere Ebenen 304
Anfordern von Zertifikaten für interne Verbindungen 306
Verwenden von Platzhalterzertifikaten 306

Anhang C Beispiele für die Konfiguration des Netzwerkzugriffs

Konfigurationsbeispiele 308
Konfigurieren der LDAP-Authentifizierung und -Autorisierung:. 309
Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung. 309
Konfigurieren des Access Gateways zur Unterstützung des Zugriffs auf die internen Netzwerkressourcen 315
Szenario für das Erstellen von Gastkonten mit der Liste „Local Users“. 325
Erstellen eines Authentifizierungsbereichs für Gastbenutzer. 327
Erstellen lokaler Benutzer 328
Erstellen und Zuweisen einer Netzwerkressource für die Standardbenutzergruppe 328
Szenario für das Konfigurieren der lokalen Autorisierung für lokale Benutzer . .329

Anhang D Problembehandlung beim Access Gateway

Problembehandlung bei Webinterface-Verbindungen. 331
Das Webinterface wird angezeigt, ohne dass Anmeldeinformationen eingegeben wurden 331
Nach dem Anmelden werden keine Anwendungen angezeigt. 331
Benutzer werden zu einer Anmeldeseite geleitet, auf der sie zum Starten des Secure Access Clients aufgefordert werden 332

Sonstige Probleme 333
Lizenzdatei stimmt nicht mit dem Access Gateway überein 333
Definieren von Subnetzeinschränkungen für zugängliche Netzwerke 333
VMWare 333
ICMP-Übertragungen 334
Ping-Befehl 334
LDAP-Authentifizierung. 334
Endpunktrichtlinien 334
Netzwerkressourcen 334
Kioskverbindungen 334
Internes Failover 335
Zertifikatsignierung 335
Zertifikatsperrlisten 335
Netzwerkmeldungen an nicht vorhandene IP-Adressen. 336
Das Access Gateway startet nicht und die serielle Konsole ist leer 336
Zugriff auf das Administration Tool nicht möglich 336
Kommunikation zwischen Geräten und dem Access Gateway nicht möglich 336
Verwenden von Strg+Alt+Entf zum Neustarten des Access Gateways nicht möglich 337
Sitzungen mit SSL Version 2 und Zertifikatketten auf mehreren Ebenen. . . .337
H.323-Protokoll 337
Zertifikate mit 512-Bit-Schlüsselpaaren 337
Laufwerkszuordnung kann nicht mit einer Anwendungsrichtlinie eingeschränkt werden 337
Secure Access Client. 338
Secure Access Client-Verbindungen mit Windows XP 338
DNS-Namensauflösung mit Namensdienstanbietern 338
Funktion zum automatischen Aktualisieren 338
Von Windows Server 2003-Computern ausgehende Clientverbindungen . . .338
NTLM-Authentifizierung 339
WINS-Einträge 339
Verwendung von Drittanbieter-Clientsoftware 339

KAPITEL 1

Einführung

In diesem Kapitel werden die Zielgruppe des *Citrix Access Gateway-Administratorhandbuchs*, der Aufbau dieses Handbuchs und die verwendeten typografischen Konventionen beschrieben.

Hinweise zur Benutzung dieses Handbuchs

Dieses Benutzerhandbuch richtet sich an Systemadministratoren, die mit der Installation und Konfiguration des Access Gateways betraut wurden. Dabei wird davon ausgegangen, dass das Access Gateway mit einem vorhandenen Netzwerk verbunden ist und dass der Administrator über die notwendigen Kenntnisse zum Konfigurieren dieses Netzwerks verfügt.

Bei den Konfigurationsschritten in diesem Dokument wird vorausgesetzt, dass das Access Gateway als eigenständige Anwendung bereitgestellt wird und dass Benutzer eine direkte Verbindung zum Access Gateway herstellen.

Dieses Benutzerhandbuch enthält auch Informationen, wie Sie das Access Gateway für die Zusammenarbeit mit Citrix Presentation Server und Access Gateway Advanced Edition konfigurieren. Weitere Informationen finden Sie unter „Bereitstellen von Zugriff auf veröffentlichte Anwendungen“ auf Seite 193 und „Bereitstellen von Access Gateway Advanced Edition“ auf Seite 37.

Typografische Konventionen

In der Access Gateway-Dokumentation werden die folgenden typografischen Konventionen für Menüs, Befehle, Tasten und Objekte in der Benutzeroberfläche des Programms verwendet:

Konvention	Bedeutung
Fettdruck	Befehle, Namen von Benutzeroberflächenobjekten, z. B. Textfelder und Optionsschaltflächen, sowie Benutzereingaben.
Kursiv	Platzhalter für Informationen oder Parameter, die Sie eingeben müssen. *Dateiname* in einem Verfahren bedeutet z. B., dass Sie den tatsächlichen Namen einer Datei eingeben müssen. Außerdem werden neue Begriffe sowie die Titel von Dokumentationen in Kursivschrift angegeben.
%SystemRoot%	Das Windows-Systemverzeichnis, das WTSRV, WINNT, WINDOWS oder ein anderer Verzeichnisname sein kann, den Sie bei der Installation von Windows angegeben haben.
`Nicht-proportional`	Text, der in einer Textdatei angezeigt wird.
{geschweifte Klammern}	Eine Reihe von Elementen, von denen eines in Befehlsanweisungen erforderlich ist. Zum Beispiel bedeutet **{ ja | nein }**, dass Sie **ja** oder **nein** eingeben müssen. Die geschweiften Klammern selbst müssen nicht eingegeben werden.
[eckige Klammern]	Optionale Elemente in Befehlsanweisungen. Zum Beispiel bedeutet [**/ping**], dass Sie **/ping** zusammen mit dem Befehl eingeben können. Geben Sie die eckigen Klammern selbst nicht mit ein.
| (vertikaler Strich)	Ein Trennzeichen zwischen Elementen in geschweiften oder eckigen Klammern in Befehlsanweisungen. Beispiel: **{ /hold | /release | /delete }** bedeutet, dass Sie **/hold** oder **/release** oder **/delete** eingeben.
… (Auslassung)	Sie können das vorherige Element bzw. die vorherigen Elemente in Befehlsanweisungen wiederholen. Zum Beispiel bedeutet **/route:***Gerätename*[,…], dass Sie zusätzliche *Gerätenamen* eingeben können, die durch Kommas getrennt werden.

Service und technischer Support

Citrix bietet technischen Support hauptsächlich durch Citrix Solution Advisors an. Unsere Citrix Solution Advisor-Partner verfügen über entsprechendes Training und bieten unseren Kunden ein hohes Niveau an Support. Wenden Sie sich zuerst an Ihren Vertragshändler oder suchen Sie unter http://support.citrix.com/ nach dem nächstgelegenen CSN-Partner.

Zusätzlich zum CSN-Programm bietet Citrix im Knowledge Center eine Reihe von webbasierten Selbstbedienungstools für den technischen Support. Das Knowledge Center finden Sie unter http://support.citrix.com/. Das Knowledge Center bietet Folgendes:

- Eine Knowledge Base mit technischen Lösungen zur Unterstützung der Citrix Umgebung
- Eine Onlinebibliothek der Produktdokumentation
- Interaktive Support-Foren für jedes Citrix Produkt
- Zugang zu den neuesten Hotfixes und Service Packs
- Security Bulletins
- Onlineproblemmeldung und -verfolgung (für Organisationen mit gültigen Supportverträgen)

Eine andere Supportquelle, Citrix Preferred Support Services, bietet eine Reihe von Optionen, sodass Sie den Grad und die Art von Support für die Citrix Produkte in Ihrer Organisation anpassen können.

Subscription Advantage

Ihr Produkt schließt das Abonnement Subscription Advantage für ein Jahr ein. Citrix Subscription Advantage bietet eine einfache Möglichkeit, stets die aktuellen Softwareversionen und Informationen für Ihre Citrix Produkte zu haben. Abonnenten erhalten nicht nur automatisch Zugriff auf den Download der neuesten Feature Release-Versionen, Softwareupgrades und Erweiterungen, die während der Laufzeit des Abonnements verfügbar werden, sondern haben auch bevorzugten Zugang zu wichtigen technischen Informationen von Citrix.

Die Dokumentation ist auch von der Citrix Website erhältlich: http://www.citrix.com/services/ (klicken Sie auf **Subscription Advantage**). Weitere Informationen erhalten Sie auch von Ihrem Vertragshändler, Citrix Customer Care oder einem Mitglied des Citrix Solutions Advisors-Programms.

Knowledge Center-Watches

Im Citrix Knowledge Center haben Sie die Möglichkeit, sogenannte *Watches* zu konfigurieren. Mit diesen Watches werden Sie benachrichtigt, wenn das Thema, für das Sie sich interessieren, aktualisiert wurde. Die Watches helfen Ihnen dabei, stets auf dem Laufenden zu bleiben, wenn es in der Knowledge Base und in den Foren neue Informationen gibt. Sie können Watches für Produktkategorien, Dokumenttypen, einzelne Dokumente sowie für Forum-Produktkategorien und einzelne Forenthemen einrichten.

Um eine Updatebenachrichtigung einzurichten, melden Sie sich bei der Citrix Support-Website an: http://support.citrix.com. Klicken Sie dann oben rechts auf **My Watches** und folgen Sie den Anweisungen.

Schulung und Zertifizierung

Citrix bietet eine Reihe von unterrichteten (ILT, engl. instructor led training) und webbasierten Kursen (WBT, engl. web-based training). Die von einem Schulungsleiter durchgeführten ILT-Kurse werden von Citrix Authorized Learning Centers (CALCs) angeboten. CALCs bieten hochwertige Schulungen mit den professionellen Schulungsmaterialien von Citrix. Viele diese Kurse bereiten auf eine Zertifizierung vor.

Webbasierte Schulungskurse werden auch von CALCs, Wiederverkäufern und über die Website von Citrix angeboten.

Informationen zu Programmen und Courseware für Citrix Schulungen und Zertifizierungen finden Sie unter http://www.citrix.com/edu/.

Literaturhinweise

Weitere Informationen zu Access Gateway finden Sie in den folgenden Dokumenten:

- *Installationsübersicht für Citrix Access Gateway Standard Edition*
- *Citrix Access Gateway Standard Edition Pre-Installation Checklist*
- Citrix Access Gateway Standard Edition Readme

Einführung in das Citrix Access Gateway

Citrix Access Gateway ist eine universelle SSL-VPN-Lösung, die einen sicheren zentralen Zugang zu allen Informationsressourcen in der Organisation – gleich ob Daten- oder Sprachinformationen – ermöglicht. Die Lösung vereint die Vorteile von IPsec und SSL VPN ohne die mit diesen Verfahren verbundene kostenintensive und aufwändige Implementierung und Wartung. Das Access Gateway ist mit jeder Firewall kompatibel und unterstützt alle Anwendungen sowie Protokolle. Es lässt sich schnell, einfach und kostengünstig einrichten und kann über einen über das Web bereitgestellten, sich automatisch aktualisierenden Client gewartet werden. Die Benutzer kommen in den Genuss eines konsistenten, den üblichen Gewohnheiten im Firmenbüro entsprechenden Benutzererlebnisses mit „Always-on"-Konnektivität und erhalten einen integrierten Client mit Wurmblockierungsfunktion sowie integrierter Endpunktprüfung. Das Citrix Access Gateway ermöglicht den sicheren Remotezugriff auf die Organisationsressourcen in einem einzigen Produkt und lässt sich schnell und einfach bereitstellen.

Mit dem Access Gateway erhalten Remotebenutzer nahtlosen und sicheren Zugriff auf autorisierte Anwendungen und Netzwerkressourcen. Remotebenutzer können mit Dateien auf Netzlaufwerken, E-Mail, Intranetsites und Anwendungen so arbeiten, als befänden sie sich weiterhin innerhalb der Firewall der Organisation.

Die folgenden Themen bieten einen Überblick über das Access Gateway:

- Access Gateway-Technologien
- Access Gateway-Betriebsmodi
- Neue Funktionen

Access Gateway-Technologien

Das Access Gateway lässt sich schnell und einfach bereitstellen und verwalten. Es wird dabei in den meisten Fällen hinter der Firewall oder in der DMZ platziert. Es werden aber auch komplexere Bereitstellungen unterstützt, z. B. bei Verwendung eines Server Load Balancers oder einer Double-Hop-DMZ.

Wenn das Access Gateway zum ersten Mal gestartet wird, müssen Sie mit dem Access Gateway Administration Tool die für Ihr Unternehmensnetzwerk geltenden Grundeinstellungen konfigurieren. Dazu gehören die IP-Adresse, die Subnetzmaske, die IP-Adresse des Standardgateways und die DNS-Adresse. Sobald die Grundeinstellungen konfiguriert wurden und eine Verbindung mit dem Netzwerk hergestellt wurde, können Sie die Einstellungen konfigurieren, die für den Einsatz dieses konkreten Access Gateway-Geräts gelten sollen. Dazu gehören die Optionen für die Authentifizierung, die Autorisierung und die gruppenbasierte Zugriffssteuerung, der Kioskmodus, die Endpunktressourcen und -richtlinien, die Portalseiten sowie die IP-Pools.

Weitere Informationen zum Installieren des Access Gateways finden Sie im Handbuch *Installationsübersicht für Citrix Access Gateway Standard Edition* oder unter „Erstmalige Installation des Access Gateways“ auf Seite 39.

Access Gateway-Betriebsmodi

Das Access Gateway kann auf vier verschiedene Arten verwendet werden:

Verbindungen nur über das Gerät: In diesem Szenario wird das Access Gateway als eigenständiges Gerät in der DMZ installiert. Benutzer stellen mit dem Secure Access Client direkt eine Verbindung zum Access Gateway her und erhalten so Zugriff auf Netzwerkressourcen, z. B. E-Mail- und Webserver.

Verbindungen mit dem Webinterface und Citrix Presentation Server: In diesem Szenario melden sich Benutzer am Webinterface an und werden dann mit ihren Anwendungen auf Citrix Presentation Server verbunden. Je nachdem wie das Access Gateway mit Presentation Server bereitgestellt wurde, können Benutzer Verbindungen nur mit den Citrix Presentation Server Clients, dem Secure Access Client oder mit beiden Clients gleichzeitig herstellen. Weitere Informationen hierzu finden Sie unter „Bereitstellen von Zugriff auf veröffentlichte Anwendungen“ auf Seite 193.

Verbindungen mit Access Gateway Advanced Edition: In diesem Szenario ist das Access Gateway in der DMZ installiert. Anfängliche TCP/IP-Einstellungen für werden während der Installation des Geräts konfiguriert. Erweiterte Einstellungen für die Verwaltung des Access Gateways werden mit der Access Management Console konfiguriert, die Teil von Access Gateway Advanced Edition ist. Weitere Informationen finden Sie unter „Bereitstellen von Access Gateway Advanced Edition“ auf Seite 37 oder im *Administratorhandbuch für Citrix Access Gateway Advanced Edition*.

Hinweis: Beim Bereitstellen von Access Gateway Advanced Edition muss das Gerät die einzige Komponente in der DMZ sein, die mit der Access-Serverfarm kommuniziert. Access Gateway Advanced Edition kann nicht mit Secure Gateway zusammenarbeiten.

Verbindungen im Kioskmodus: Das Access Gateway verfügt darüber hinaus auch über einen Kioskmodus, der eine VNC-artige (Virtual Network Computing) Verbindung zum Access Gateway öffnet. Der Kioskmodus kann freigegebene Netzlaufwerke, eine Vielzahl von integrierten Clients, Server mit Windows-Terminaldiensten (Remotedesktop) und Clientanwendungen beinhalten. Weitere Informationen über den Kioskmodus finden Sie unter „Verbindungen im Kioskmodus“ auf Seite 157.

Funktionen des Access Gateways

Das Access Gateway übernimmt die folgenden Funktionen:

- Authentifizierung
- Terminierung verschlüsselter Sitzungen
- Zugriffssteuerung (auf der Basis von Berechtigungen)
- Weiterleitung des Datenverkehrs (wenn die ersten drei Funktionen erfüllt wurden)

Als eigenständiges Gerät in der DMZ arbeitet das Access Gateway folgendermaßen:

- Ein Remotebenutzer lädt den Secure Access Client herunter, indem er eine Verbindung zu einer sicheren Webadresse herstellt und seine Authentifizierungsinformationen eingibt.
- Nach dem Herunterladen des Secure Access Clients meldet sich der Benutzer an. Wenn die Authentifizierung des Benutzers erfolgreich war, richtet das Access Gateway einen sicheren Tunnel ein.
- Sobald der Remotebenutzer versucht, über den VPN-Tunnel auf die Netzwerkressourcen zuzugreifen, verschlüsselt der Secure Access Client den gesamten Netzwerkverkehr, der für das Intranet der Organisation bestimmt ist, und leitet die Pakete an das Access Gateway weiter.
- Das Access Gateway fungiert als Endpunkt des SSL-Tunnels (terminiert den Tunnel), akzeptiert den eingehenden Verkehr, der für das private Netzwerk bestimmt ist, und leitet den Verkehr an das private Netzwerk weiter. Das Access Gateway sendet den Verkehr über einen sicheren Tunnel zum Remotecomputer zurück.

Neue Funktionen

Diese Version des Access Gateways enthält folgende neue Funktionen:

Double-Hop-DMZ-Unterstützung für Citrix Presentation Server: Durch die Bereitstellung des Access Gateways in einer Double-Hop-DMZ schaffen Sie einen zentralen Zugriffspunkt auf eine Serverfarm, die sich in einem internen Netzwerk befindet. In dieser Konfiguration müssen Sie zwei Access Gateway-Geräte bereitstellen: ein Gerät in der ersten Stufe der DMZ und das zweite in der zweiten Stufe der DMZ. Das Access Gateway in der zweiten Stufe der DMZ fungiert als Proxy für ICA-Verkehr durch die zweite DMZ. Weitere Informationen über die Bereitstellung des Access Gateways in einer Double-Hop-Konfiguration finden Sie unter „Bereitstellen des Access Gateways in einer Double-Hop-DMZ“ auf Seite 223.

Konfigurierbare symmetrische Verschlüsselung: Sie können die Verschlüsselung festlegen, die das Access Gateway für die symmetrische Datenverschlüsselung bei einer SSL-Verbindung verwendet. Sie können einer dieser drei Verschlüsselungen wählen:

- RC4 128 Bit, MD5/SHA
- 3DES, SHA
- AES 128/256 Bit, SHA

Automatische Erkennung von Proxyservereinstellungen: In diesem Release ermittelt der Secure Access Client automatisch die im Betriebssystem festgelegten Proxyservereinstellungen.

Secure Access Client-Verbindungen: Der Secure Access Client in dieser Version kann Verbindungen zu früheren Versionen des Access Gateways herstellen Außerdem können frühere Versionen des Secure Access Clients Verbindungen zu dieser Version des Access Gateways herstellen, wenn dies auf der Registerkarte **Global Cluster Policies** eingestellt ist.

Automatische Portumleitung: Sie können das Access Gateway so konfigurieren, dass unsichere HTTP-Verbindungsversuche auf Port 80 vom Access Gateway automatisch an sichere HTTPS-Verbindungsversuche auf Port 443 (oder einen anderen vom Administrator festgelegten Port) weitergeleitet werden.

Deaktivieren der Desktopfeigabe: Sie können die Desktopfreigabefunktion des Secure Access Clients für eine Benutzergruppe deaktivieren. Mit dieser Funktion können Benutzer eine Liste aller anderen Benutzer anzeigen, die gerade angemeldet sind. Wenn diese Funktion zu Bedenken wegen des Datenschutzes in Ihrem Unternehmen führt, können Sie die Desktopfreigabe deaktivieren, um eine bestimmte Benutzergruppe am Anzeigen der Liste der angemeldeten Benutzer zu hindern.

Zusätzliche Kontrolle über Secure Access Client-Verbindungen: Sie können den Secure Access Client so konfigurieren, dass er die Verbindung zum Access Gateway trennt, wenn während eines festgelegten Zeitraums keine Benutzeraktivität stattfindet. Sie können eine Trennung der Clientverbindung auch erzwingen, wenn die Verbindung für eine bestimmte Zeit aktiv bleibt oder wenn das Access Gateway keine Tastatur- oder Mausaktivitäten erkennt.

Deaktivieren des Kioskmodus: In dieser Version können Sie den Kioskmodus für Clientverbindungen deaktivieren. Wenn der Kioskmodus deaktiviert ist, sehen Benutzer keinen Kiosk-Link auf der der Webportalseite. Benutzer dürfen sich nur mit dem vollen Secure Access Client oder den Citrix Presentation Server Clients anmelden.

Festlegen mehrerer Ports und Portbereiche für Netzwerkressourcen: In dieser Version können Sie Portbereiche konfigurieren. Sie haben vier Optionen beim Konfigurieren der Ports, die das Access Gateway zum Herstellen einer Verbindung zu internen Netzwerkressourcen verwendet. Sie können einen einzigen Port, mehrere einzelne Ports, einen Portbereich oder alle Ports festlegen.

Aktualisierte Lizenzierung: Die Lizenzierung für das Access Gateway wurde geändert, damit ein Access Gateway als Lizenzserver für alle bereitgestellten Geräte fungieren kann. Lizenzen werden auf einem Access Gateway installiert und die anderen Geräte im Netzwerk werden so konfiguriert, dass sie ihre Lizenzen von dem primären Access Gateway erhalten.

VoIP-Softphone-Unterstützung: Das Access Gateway unterstützt VoIP-Softphones von Avaya, Nortel und Cisco.

Bearbeiten der HOSTS-Datei: Sie können die HOSTS-Datei auf dem Access Gateway über die Benutzeroberfläche des Administration Tools bearbeiten. Das Access Gateway verwendet die HOSTS-Datei zusammen mit DNS-Servern, um DNS-Auflösung zum Übersetzen von Hostnamen in IP-Adressen zu zwingen.

Ausführen von in der Microsoft Active Directory-Gruppenrichtlinie festgelegten Anmeldeskripten: Das Access Gateway unterstützt die Ausführung von Windows Anmeldeskripten, die in der Microsoft Active Directory-Gruppenrichtlinie festgelegt sind. Benutzer müssen sich erfolgreich beim Secure Access Client authentifizieren, bevor die Anmeldeskripte ausgeführt werden können.

Unterstützung für NTLM-Authentifizierung und -Autorisierung: Wenn Ihre Umgebung Windows NT 4.0-Domänencontroller enthält, kann das Access Gateway Benutzer gegen die Domänenbenutzerkonten auf dem Windows NT-Server authentifizieren. Das Access Gateway kann Benutzer basierend auf den Gruppenmitgliedschaften der Benutzer auf dem Windows NT 4.0-Domänencontroller auch für den Zugriff auf interne Netzwerkressourcen autorisieren.

Challenge/Response wurde der RADIUS-Benutzerauthentifizierung hinzugefügt: Das Access Gateway unterstützt jetzt Challenge/Response-Tokenauthentifizierung mit Modi für neue PIN-Nummer und nächstem Token, wenn RSA SedurID-Authentifizierung mit RADIUS verwendet wird.

SafeWord PremierAccess geändert, damit standardbasierte RADIUS-Token-Benutzerauthentifizierung unterstützt wird: Die proprietäre PremierAccess-Konfigurationsdatei wurde entfernt und durch RADIUS-Serverunterstützung ersetzt. Verbliebene SafeWord PremierAccess-Bereiche werden beim Upgrade des Access Gateways auf Version 4.5 konvertiert. SafeWord-Authentifizierung wird mit RADIUS-ähnlichen Parametern konfiguriert.

Aktualisiertes Menü in der seriellen Konsole: Die serielle Konsole enthält neue Menüeinträge, mit denen Sie das Access Gateway-Administratorkennwort ändern, Duplexmodus und Netzwerkadaptergeschwindigkeit festlegen und das Standardzertifikat, das zum Lieferumfang des Access Gateways gehört, wiederherstellen können.

Planen der Bereitstellung

In diesem Kapitel werden Bereitstellungsszenarien für das Access Gateway vorgestellt.

Sie können das Access Gateway am Rand des internen Netzwerks (Intranet) Ihres Unternehmens bereitstellen, sodass ein zentraler Zugriffspunkt auf alle Servern, Anwendungen und andere Netzwerkressourcen im internen Netzwerk entsteht. Alle Remotebenutzer müssen eine Verbindung zum Access Gateway herstellen, bevor sie auf die Ressourcen im internen Netzwerk zugreifen können.

Dieses Kapitel umfasst die folgenden vier Abschnitte:

- Bereitstellen des Access Gateways.
- Bereitstellen des Access Gateways mit Citrix Presentation Server. In diesem Abschnitt wird die Bereitstellung des Access Gateways mit einer Serverfarm erläutert. Sie können das Access Gateway wahlweise in einer Single- oder Double-Hop-DMZ-Konfiguration bereitstellen.
- Bereitstellen weiterer Access Gateway-Geräte für Lastausgleich und Failover.
- Bereitstellen des Access Gateways mit Access Gateway Advanced Edition.

Bereitstellen des Access Gateways

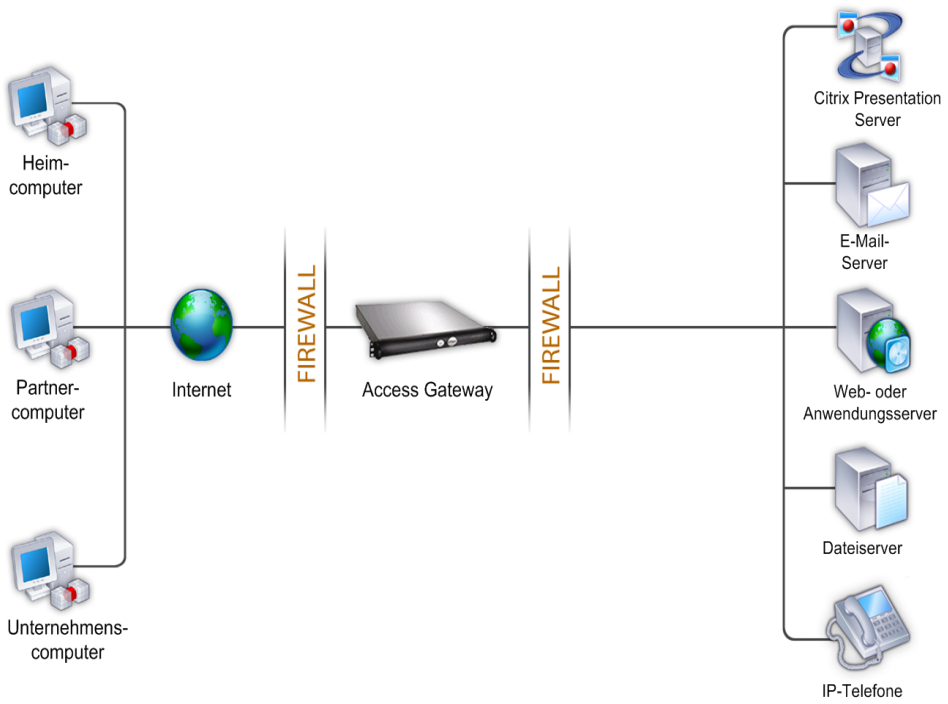
In diesem Abschnitt werden die folgenden Access Gateway-Bereitstellungen erläutert:

- Bereitstellen des Access Gateways in der demilitarisierten Zone (DMZ) des Netzwerks
- Bereitstellen des Access Gateways in einem sicheren Netzwerk, das keine DMZ besitzt
- Bereitstellen weiterer Access Gateway-Geräte für Lastausgleich und Failover

Access Gateway in der DMZ des Netzwerks

Viele Unternehmen schützen ihr internes Netzwerk mithilfe einer DMZ. Eine DMZ ist ein Subnetz, das zwischen dem sicheren internen Netzwerk des Unternehmens und dem Internet (oder einem externen Netzwerk) liegt. Wird das Access Gateway in der DMZ bereitgestellt, greifen die Benutzer über den Secure Access Client, die Citrix Presentation Server Clients oder den Kioskclient auf das Access Gateway zu.

Hinweis: Weitere Informationen zur Bereitstellung des Access Gateways in der DMZ, um Zugriff auf eine Serverfarm zu ermöglichen, finden Sie unter „Bereitstellen des Gateways mit Citrix Presentation Server“ auf Seite 28.



Access Gateway in der DMZ

Installieren des Access Gateways in der DMZ

In dieser Konfiguration wird das Access Gateway in der DMZ installiert und so konfiguriert, dass eine Verbindung sowohl zum Internet als auch zum internen Netzwerk hergestellt wird. Zur Installation und Konfiguration folgen Sie den Anweisungen unter „Erstmalige Installation des Access Gateways“ auf Seite 39.

Access Gateway-Konnektivität in der DMZ

Wenn Sie das Access Gateway in der DMZ bereitstellen, müssen die Clientverbindungen die Firewall überwinden, um eine Verbindung zum Access Gateway herstellen zu können. Standardmäßig erfolgt diese Verbindung mit SSL (Secure Sockets Layer) an Port 443. Damit diese Verbindung möglich ist, müssen Sie die Verwendung von SSL an Port 443 durch die erste Firewall zulassen.

Hinweis: Sie können den Port ändern, über den die Clients eine Verbindung zum Access Gateway aufbauen. Bearbeiten Sie hierzu die Porteinstellung im Administration Tool. Weitere Informationen zu dieser Porteinstellung finden Sie unter „Konfigurieren der TCP/IP-Einstellungen mit Netzwerkkabeln“ auf Seite 45.

Das Access Gateway entschlüsselt die SSL-Verbindungen vom Client und baut stellvertretend für den Client eine Verbindung zu den Netzwerkressourcen hinter der zweiten Firewall auf. Die Ports, die für den Durchgang durch die zweite Firewall geöffnet sein müssen, sind abhängig von den Netzwerkressourcen, für deren Zugriff die externen Benutzer autorisiert sind.

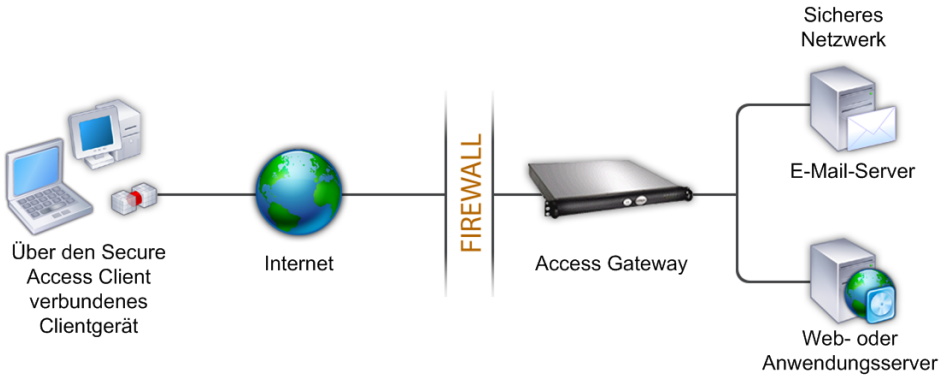
Wenn Sie beispielsweise die externen Benutzer für den Zugriff auf einen Webserver im internen Netzwerk autorisieren und der Server Port 80 nach HTTP-Verbindungen abhört, muss entsprechend HTTP an Port 80 durch die zweite Firewall zugelassen werden. Stellvertretend für die externen Clients stellt das Access Gateway die Verbindung durch die zweite Firewall zum HTTP-Server im internen Netzwerk her.

Mit den Verwaltungstools des Access Gateways hören außerdem die folgenden Ports nach Verbindungen ab:

- Port 9001: Über diesen Port erfolgen Verbindungen zum Administration Portal.
- Port 9002: Über diesen Port erfolgen Verbindungen zum Administration Tool.

Access Gateway in einem sicheren Netzwerk

Sie können das Access Gateway im sicheren Netzwerk installieren. In diesem Szenario befindet sich in der Regel eine Firewall zwischen dem Internet und dem sicheren Netzwerk. Das Access Gateway befindet sich innerhalb der Firewall und steuert den Zugriff auf die Netzwerkressourcen.



Access Gateway in einem sicheren Netzwerk

Access Gateway-Konnektivität in einem sicheren Netzwerk

Wird ein Access Gateway im sicheren Netzwerk bereitgestellt, müssen die Secure Access Client- oder Kioskclient-Verbindungen die Firewall überwinden, um eine Verbindung zum Access Gateway herstellen zu können. Standardmäßig erfolgt diese Verbindung bei beiden Clients mithilfe des SSL-Protokolls an Port 443. Damit diese Verbindung möglich ist, müssen Sie Port 443 in der Firewall öffnen.

Hinweis: Sie können den Port ändern, über den die Clients eine Verbindung zum Access Gateway aufbauen. Bearbeiten Sie hierzu die Porteinstellung im Administration Tool. Weitere Informationen zu dieser Porteinstellung finden Sie unter „Konfigurieren der TCP/IP-Einstellungen mit Netzwerkkabeln“ auf Seite 45.

Überlegungen zur Sicherheit

Beim Planen jeder Access Gateway-Bereitstellung sind gewisse grundlegende Sicherheitsaspekte im Zusammenhang mit Zertifikaten, mit der Authentifizierung und mit der Autorisierung zu beachten.

Konfigurieren der sicheren Zertifikatverwaltung

Standardmäßig enthält das Access Gateway ein selbst signiertes SSL-Serverzertifikat, mit dem das Access Gateway in der Lage ist, SSL-Handshakes zu verarbeiten. Für Testbereitstellungen sind selbst signierte Zertifikate durchaus angemessen; für den Einsatz in Produktionsumgebungen reichen diese Zertifikate jedoch nicht aus.

Citrix rät daher, vor der Bereitstellung des Access Gateways in einer Produktionsumgebung ein signiertes SSL-Serverzertifikat von einer anerkannten Zertifizierungsstelle einzuholen und auf das Access Gateway hochzuladen.

Wird das Access Gateway in einer Umgebung bereitgestellt, in der es als Client bei SSL-Handshakes fungiert (also verschlüsselte Verbindungen zu einem anderen Server einleitet), muss außerdem ein vertrauenswürdiges Stammzertifikat auf dem Access Gateway installiert werden. Weitere Informationen zu Stammzertifikaten finden Sie unter „Installieren von Stammzertifikaten auf dem Access Gateway“ auf Seite 60.

Wenn Sie beispielsweise das Access Gateway mit Citrix Presentation Server und mit dem Webinterface installieren, können Sie Verbindungen vom Access Gateway zum Webinterface mit SSL verschlüsseln. Bei dieser Konfiguration muss ein vertrauenswürdiges Stammzertifikat auf dem Access Gateway installiert werden.

Weitere Informationen finden Sie unter „Erstellen und Installieren von Zertifikaten“ auf Seite 55 und „Sichern von Verbindungen mit digitalen Zertifikaten“ auf Seite 291.

Unterstützung bei der Authentifizierung

Sie können das Access Gateway so konfigurieren, dass die Benutzer authentifiziert werden und damit die Zugriffsstufe (Autorisierungsstufe) der Benutzer auf die Netzwerkressourcen im internen Netzwerk gesteuert wird.

Vor der Bereitstellung des Access Gateways sollten Sie alle Unternehmensverzeichnisse und die Authentifizierungsserver in der Netzwerkumgebung einrichten, die zur Unterstützung einer der folgenden Authentifizierungsarten erforderlich sind:

- LDAP
- RADIUS
- RSA SecurID
- NTLM
- SafeWord-Produkte von Secure Computing

Falls Ihre Umgebung die oben genannten Authentifizierungsarten nicht unterstützt oder nur wenige Remotebenutzer vorhanden sind, können Sie eine Liste lokaler Benutzer auf dem Access Gateway anlegen und das Access Gateway so konfigurieren, dass die Benutzer anhand dieser lokalen Liste authentifiziert werden. Bei dieser Konfiguration ist es nicht nötig, Benutzerkonten in einem separaten, externen Verzeichnis anzulegen.

Weitere Informationen zur Authentifizierung und Autorisierung finden Sie unter „Beispiele für die Konfiguration des Netzwerkzugriffs“ auf Seite 307 und „Konfigurieren der Authentifizierung und Autorisierung“ auf Seite 77.

Bereitstellen des Gateways mit Citrix Presentation Server

Wird das Access Gateway mit dem Ziel bereitgestellt, für sicheren Remotezugriff auf Citrix Presentation Server zu sorgen, ermöglicht das Access Gateway gemeinsam mit dem Webinterface und der Secure Ticket Authority (STA) den Zugriff auf veröffentlichte Anwendungen und Ressourcen, die auf einer Serverfarm gehostet werden.

In diesem Abschnitt werden die Grundlagen bei der Bereitstellung des Access Gateways mit einer Serverfarm erläutert. Weitere Informationen zu dieser Bereitstellungsform finden Sie unter „Bereitstellen von Zugriff auf veröffentlichte Anwendungen“ auf Seite 193.

Die Konfiguration des Netzwerks Ihres Unternehmens bestimmt die Position, an der Sie das Access Gateway bereitstellen, wenn es zusammen mit einer Serverfarm genutzt werden soll. Hierbei stehen zwei Optionen zur Auswahl:

- Ist das interne Netzwerk in Ihrem Unternehmen mit einer einzelnen DMZ geschützt, stellen Sie das Access Gateway direkt in der DMZ bereit.
- Ist das interne Netzwerk in Ihrem Unternehmen dagegen mit zwei DMZs geschützt, stellen Sie je ein Access Gateway in den beiden Netzwerksegmenten in einer Double-Hop-DMZ-Konfiguration bereit. Weitere Informationen zur Bereitstellung des Access Gateways in einer Double-Hop-DMZ finden Sie unter „Bereitstellen des Access Gateways in einer Double-Hop-DMZ“ auf Seite 223.

Bereitstellen des Gateways in der DMZ mit Citrix Presentation Server

Die Bereitstellung des Access Gateways in der DMZ ist die am häufigsten verwendete Konfiguration, wenn das Access Gateway mit einer Serverfarm zusammenarbeitet.

In dieser Konfiguration bildet das Access Gateway einen zentralen Zugriffspunkt für die Webbrowser und die Presentation Server Clients, die über das Webinterface auf die veröffentlichten Ressourcen zugreifen.

Access Gateway und Webinterface in der DMZ. Auf den Computern im sicheren Netzwerk wird Citrix Presentation Server ausgeführt.

Bei der Bereitstellung des Access Gateways in der DMZ stehen für den Remotezugriff auf eine Serverfarm drei Möglichkeiten zur Auswahl:

Bereitstellen des Webinterface hinter dem Access Gateway in der DMZ: In dieser Konfiguration werden sowohl das Access Gateway als auch das Webinterface in der DMZ bereitgestellt. Die anfängliche Clientverbindung geht zum Access Gateway und wird dann an das Webinterface umgeleitet.

Ein Beispiel für diese Konfiguration finden Sie unter „Herstellen einer sicheren Verbindung zur Serverfarm“ auf Seite 30.

Bereitstellen des Access Gateways parallel zum Webinterface in der DMZ: In dieser Konfiguration werden sowohl das Access Gateway als auch das Webinterface in der DMZ bereitgestellt; die anfängliche Clientverbindung geht jedoch nicht zum Access Gateway, sondern zum Webinterface.

Das Webinterface erzeugt in Interaktion mit der Secure Ticket Authority eine ICA-Datei, mit der sichergestellt wird, dass der Datenverkehr von den Presentation Server Clients durch das Access Gateway an einen Computer in der Serverfarm weitergeleitet wird, auf dem Presentation Server ausgeführt wird.

Wenn Sie das Webinterface parallel zum Access Gateway in der DMZ bereitstellen, muss das Webinterface ein Mitglied der Windows-Domäne sein.

Bereitstellen des Access Gateways in der DMZ und Bereitstellen des Webinterface im internen Netzwerk: Bei dieser Konfiguration werden Benutzeranforderungen durch das Access Gateway authentifiziert, bevor sie an das Webinterface im sicheren Netzwerk weitergeleitet werden. Das Webinterface übernimmt nicht selbst die Authentifizierung, sondern erzeugt in Interaktion mit der Secure Ticket Authority eine ICA-Datei, mit der der ICA-Datenverkehr durch das Access Gateway an die Serverfarm weitergeleitet wird.

Weitere Informationen finden Sie unter „Bereitstellen von Zugriff auf veröffentlichte Anwendungen“ auf Seite 193.

Herstellen einer sicheren Verbindung zur Serverfarm

In diesem Abschnitt wird an einem Beispiel erläutert, wie ein in der DMZ bereitgestelltes Access Gateway in Zusammenarbeit mit dem Webinterface einen sicheren, zentralen Zugriffspunkt auf die veröffentlichten Ressourcen in einem sicheren Unternehmensnetzwerk bildet.

In diesem Beispiel gelten die folgenden Bedingungen:

- Clients aus dem Internet stellen über Presentation Server Clients eine Verbindung zum Access Gateway her.
- Das Webinterface befindet sich hinter dem Access Gateway in der DMZ. Die Clients bauen eine anfängliche Verbindung zum Access Gateway auf, die dann an das Webinterface umgeleitet wird.

- Das sichere Netzwerk enthält eine Serverfarm. Auf einem Server innerhalb dieser Serverfarm wird die Secure Ticket Authority ausgeführt und auf einem anderen Server innerhalb der Serverfarm wird der Citrix XML-Dienst ausgeführt.

Die Clients greifen mit dem folgenden Verfahren auf die Ressourcen zu, die in der Serverfarm veröffentlicht sind:

- Ein Remotebenutzer gibt die Adresse des Access Gateways in das Adressfeld eines Webbrowsers ein. Beispiel: https://www.ag.wxyco.com. Der Client versucht, diese SSL-Verbindung über Port 443 herzustellen. Diese Verbindung lässt sich nur dann aufbauen, wenn Port 443 in der Firewall geöffnet ist.
- Das Access Gateway empfängt die Verbindungsanforderung, ist jedoch so konfiguriert, dass die Anforderung an das Webinterface weitergeleitet wird.
- Das Webinterface sendet eine Anmeldeseite an den Clientbrowser.
- Der Benutzer gibt seine Anmeldeinformationen ein. Diese Anmeldeinformationen werden über das Access Gateway an das Webinterface zurückgegeben.
- Das Webinterface sendet die Anmeldeinformationen des Benutzers an den Citrix XML-Dienst, der in der Serverfarm ausgeführt wird.
- Der XML-Dienst authentifiziert die Anmeldeinformationen und sendet eine Liste der veröffentlichten Anwendungen an das Webinterface, auf die der Benutzer zugreifen darf.
- Im Webinterface wird auf einer Webseite die Liste der veröffentlichten Ressourcen angezeigt, auf die der Benutzer zugreifen darf; diese Webseite wird dann an den Client gesendet.
- Der Benutzer klickt auf den Link einer veröffentlichten Anwendung. An das Webinterface wird eine HTTP-Anforderung gesendet, aus der die ausgewählte veröffentlichte Anwendung hervorgeht.
- Das Webinterface interagiert mit dem XML-Dienst und empfängt ein Ticket, in dem der Server vermerkt ist, auf dem die veröffentlichte Anwendung ausgeführt werden soll.
- Das Webinterface sendet eine Sitzungsticketanforderung an die Secure Ticket Authority. Diese Anforderung enthält die IP-Adresse des Servers, auf dem die veröffentlichte Anwendung ausgeführt wird. Die Secure Ticket Authority speichert diese IP-Adresse und sendet das angeforderte Sitzungsticket an das Webinterface.

- Das Webinterface generiert eine ICA-Datei mit dem von der Secure Ticket Authority ausgestellten Ticket und sendet diese Datei an den Clientbrowser.

  Die vom Webinterface generierte ICA-Datei enthält den vollqualifizierten Domänennamen (FQDN) oder den DNS-Namen des Access Gateways. Hinweis: Die IP-Adresse des Servers, auf dem die angeforderte Anwendung ausgeführt wird, wird dabei dem Client gegenüber nicht offen gelegt.

- Die ICA-Datei enthält Anweisungen für den Webbrowser zum Starten des Presentation Server Clients. Der Client stellt über den in der ICA-Datei aufgeführten vollqualifizierten Domänennamen oder DNS-Namen des Access Gateways eine Verbindung zum Access Gateway her. Es kommt zum ersten SSL/TLS-Handshake, mit dem die Identität des Access Gateways ermittelt wird.

- Der Presentation Server Client sendet das Sitzungsticket an das Access Gateway und das Access Gateway wendet sich zur Überprüfung des Tickets an die Secure Ticket Authority.

- Die Secure Ticket Authority gibt die IP-Adresse des Servers, auf dem die angeforderte Anwendung ausgeführt wird, an das Access Gateway zurück.

- Das Access Gateway stellt eine TCP-Verbindung zu einem Computer her, auf dem Presentation Server ausgeführt wird.

- Das Access Gateway schließt den Verbindungs-Handshake mit dem Presentation Server Client ab und signalisiert dem Client, dass die Verbindung zum Server nun aufgebaut ist.

  Der gesamte weitere Datenverkehr zwischen dem Client und dem Server wird einfach durch das Access Gateway weitergeleitet.

  Der Datenverkehr zwischen dem Presentation Server Client und dem Access Gateway ist verschlüsselt. Der Datenverkehr zwischen dem Access Gateway und dem Server kann unabhängig davon verschlüsselt werden; standardmäßig erfolgt jedoch keine Verschlüsselung.

Bereitstellen des Access Gateways in einer Double-Hop-DMZ

Einige Unternehmen verwenden drei Firewalls zum Schutz ihrer internen Netzwerke. Diese drei Firewalls unterteilen die DMZ in zwei Bereiche, sodass ein zusätzliches Maß an Sicherheit für das interne Netzwerk erzielt wird. Diese Netzwerkkonfiguration wird als *Double-Hop-DMZ* bezeichnet.

Durch die Bereitstellung des Access Gateways in einer Double-Hop-DMZ schaffen Sie einen zentralen Zugriffspunkt auf eine Serverfarm, die sich in einem internen Netzwerk befindet. In dieser Konfiguration müssen Sie zwei Access Gateway-Geräte bereitstellen: ein Gerät in der ersten Stufe der DMZ und das zweite in der zweiten Stufe der DMZ.

Wichtig: Wird das Access Gateway in einem Double-Hop-Szenario bereitgestellt, können die Clients nur mit Citrix Presentation Server Clients auf Ressourcen in einer Serverfarm zugreifen. Der Zugriff auf Ressourcen im internen Netzwerk über den Secure Access Client ist in einem Double-Hop-DMZ-Szenario nicht möglich. Es wird lediglich der ICA-Datenverkehr unterstützt.

Zwei Access Gateway-Geräte in einer Double-Hop-DMZ

Die obige Abbildung zeigt zwei Access Gateway-Geräte in einer Double-Hop-DMZ, mit denen der Zugriff auf eine Serverfarm gesteuert wird.

Bei dieser Form der Bereitstellung übernehmen die Clients, die Access Gateway-Geräte und das Webinterface die folgenden Aufgaben:

- Benutzer aus dem Internet stellen über einen Webbrowser und einen Presentation Server Client eine Verbindung zum Access Gateway in der ersten DMZ her.
- Das Access Gateway in der ersten DMZ empfängt die Clientverbindungen und leitet diese Verbindungen an das Webinterface in der zweiten DMZ weiter. Dieses Access Gateway verarbeitet außerdem die Verbindungen von den Clients, die eine Verbindung zur Serverfarm im internen Netzwerk aufbauen.
- Das Webinterface arbeitet verschiedene Schritte mit den Webbrowser-Clients und den Komponenten des Servers ab, unter anderem mit dem XML-Dienst und der Secure Ticket Authority. Als Ergebnis dieser Interaktionen erhält der Benutzer eine Liste der veröffentlichten Anwendungen; mit den Links in dieser Liste greift der Benutzer auf die gewünschte veröffentlichte Anwendung zu.

Wichtig: Das Webinterface muss parallel zum Access Gateway in der zweiten DMZ installiert werden.

- Das Access Gateway in der zweiten DMZ fungiert als Proxy, über den der ICA-Datenverkehr die zweite DMZ überwindet und eine Verbindung zur Serverfarm im internen Netzwerk hergestellt wird. Über das Access Gateway in der zweiten DMZ kann außerdem das Access Gateway in der ersten DMZ mit der Secure Ticket Authority im internen Netzwerk kommunizieren.

Weitere Informationen zu diesen Interaktionen und den erforderlichen Konfigurationsschritten für die Bereitstellung von zwei Access Gateway-Geräten in einer Double-Hop-DMZ-Konfiguration finden Sie unter „Bereitstellen des Access Gateways in einer Double-Hop-DMZ“ auf Seite 223.

Bereitstellen weiterer Geräte für Lastausgleich und Failover

Sie können mehrere Access Gateway-Geräte in Ihrer Umgebung installieren, um damit Folgendes zu erreichen:

Skalierbarkeit: Wenn Sie viele Remotebenutzer haben, installieren Sie zusätzliche Access Gateway-Geräte, um diese Arbeitsbelastung zu bewältigen.

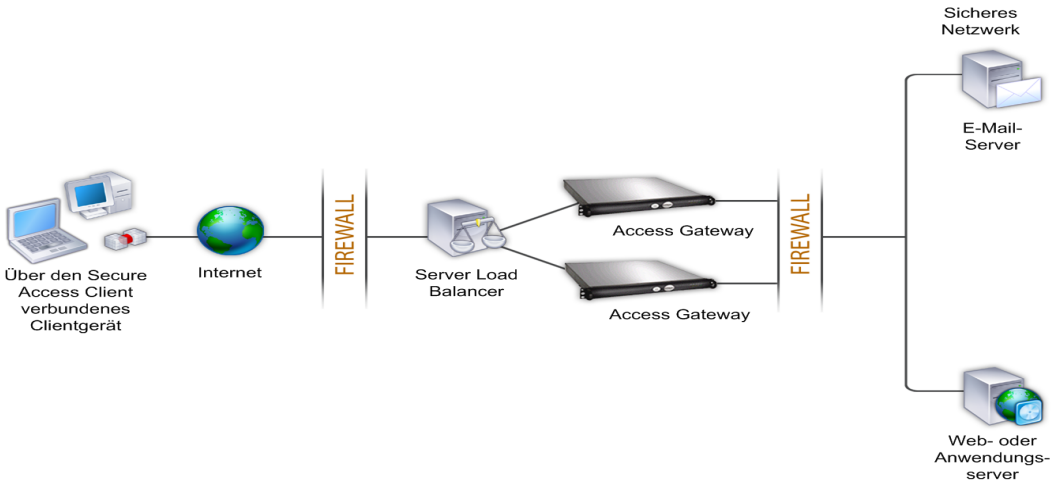
Hohe Verfügbarkeit: Als Vorsichtsmaßnahme für einen eventuellen Ausfall eines Access Gateways können Sie ein zusätzliches Access Gateway installieren und so dafür sorgen, dass das interne Netzwerk weiterhin für die Remotebenutzer verfügbar bleibt.

Hinweis: Soll lediglich eine hohe Verfügbarkeit erzielt werden, können Sie ein Access Gateway als primäres Access Gateway konfigurieren und ein oder mehrere weitere Access Gateway-Geräte als Failover-Geräte deklarieren. Bei einem Ausfall des primären Access Gateways werden die Clientverbindungen an das Failover-Access Gateway weitergeleitet. Weitere Informationen zu dieser Konfiguration finden Sie unter „Installieren zusätzlicher Access Gateway-Geräte“ auf Seite 271.

Bereitstellen von Access Gateway-Geräten hinter einem Load Balancer

Um sowohl Skalierbarkeit als auch hohe Verfügbarkeit zu unterstützen, können Sie einen Load Balancer und dann mehrere Access Gateway-Geräte hinter diesem Load Balancer installieren.

Durch die Bereitstellung mehrerer Geräte hinter einem Load Balancer können Sie eine große Anzahl Remotebenutzer unterstützen und dabei die hohe Verfügbarkeit des internen Netzwerks für die Benutzer sicherstellen.



Mehrere Access Gateway-Geräte hinter einem Load Balancer

Weitere Informationen zur Bereitstellung mehrerer Access Gateway-Geräte hinter einem Load Balancer finden Sie unter „Installieren zusätzlicher Access Gateway-Geräte“ auf Seite 271.

Bereitstellen von Access Gateway Advanced Edition

Citrix Access Gateway Advanced Edition besteht aus dem Access Gateway-Gerät und der Software Advanced Access Control.

Wenn Sie Access Gateway Advanced Edition erworben haben, müssen Sie das Access Gateway so konfigurieren, dass es mit der Advanced Access Control-Software kommunizieren kann. Legen Sie mit dem Administration Tool fest, dass die Verwaltung der Einstellungen für das oder die Gatewaycluster durch Advanced Access Control erfolgen soll. Nach der Konfiguration von Advanced Access Control können Sie mit dem Administration Tool nur noch gerätespezifische Einstellungen verwalten.

Achtung: Wenn Sie festlegen, dass Advanced Access Control das Access Gateway verwalten soll, werden die entsprechenden Einstellungen im Administration Tool deaktiviert. Wurden diese Einstellungen mit dem Administration Tool konfiguriert, bevor Sie Advanced Access Control ausgewählt haben, müssen Sie diese Einstellungen mit der Access Management Console erneut konfigurieren. Weitere Informationen zum Konfigurieren dieser Einstellungen in der Konsole finden Sie im *Administratorhandbuch für Citrix Access Gateway Advanced Edition*.

Wenn Sie die Verwaltung mit Advanced Access Control deaktivieren, werden die Einstellungen in der Access Management Console deaktiviert und die vorhandenen Konfigurationswerte werden entfernt. Die Einstellungen, die zuvor auf dem Access Gateway konfiguriert waren, werden wiederhergestellt.

So aktivieren Sie Advanced Access Control:

1. Wählen Sie auf der Registerkarte **Access Gateway Cluster** ein Access Gateway-Gerät aus und klicken Sie auf die Registerkarte **Advanced Options**.
2. Aktivieren Sie die Option **Advanced Access Control**.
3. Geben Sie im Feld **Server running Advanced Access Control** die IP-Adresse oder den vollqualifizierten Domänennamen des Servers ein, auf dem die Access Management Console ausgeführt wird.
4. Wenn die Kommunikation zwischen dem Access Gateway und dem Server, auf dem Advanced Access Control ausgeführt wird, verschlüsselt werden soll, aktivieren Sie **Secure server communication**.
5. Klicken Sie auf **Submit**.

Die Server, die so konfiguriert sind, dass sie eine Verbindung zum Access Gateway herstellen, werden unter **Servers Running Advanced Access Control** aufgelistet. Wenn Sie einen Server aus dieser Liste entfernen möchten, wählen Sie den Server aus und klicken Sie dann auf **Remove**.

Hinweis: Bei der Bereitstellung des Access Gateways mit Access Gateway Advanced Edition ist das Gerät die einzige Komponente, die sich in der DMZ befinden und mit der Access-Serverfarm kommunizieren darf. Das Secure Gateway kann nicht zusammen mit Access Gateway Advanced Edition eingesetzt werden.

Mehrere Server in einer Access-Serverfarm

Ist in der Konfiguration des Access Gateways festgelegt, dass Verbindungen mit mehreren Servern mit Access Gateway Advanced Edition aufgebaut werden sollen, wird überprüft, ob die Server tatsächlich aktiv sind, bevor das Access Gateway eine Anforderung an die Server sendet. Stellt das Access Gateway fest, dass ein Server nicht aktiv ist, wird in regelmäßigen Zeitabständen überprüft, ob der Server wieder online ist. Sie können die Zeitabstände in Sekunden angeben, in denen das Access Gateway den Server überprüft. Der Mindestzeitraum beträgt 60 Sekunden.

So legen Sie das Überprüfungsintervall für einen Server mit Advanced Access Control fest:

1. Klicken Sie auf die Registerkarte **Access Gateway Cluster** und anschließend auf die Registerkarte **Advanced Options**.
2. Geben Sie den gewünschten Zeitraum in das Feld **Retry invalid server in access server farm every** *Zeitraum in Sekunden* **seconds** ein; *Zeitraum in Sekunden* bezeichnet hierbei das Textfeld.
3. Klicken Sie auf **Set**.

KAPITEL 4

Erstmalige Installation des Access Gateways

Die Installation des Access Gateways in einer Netzwerkinfrastruktur erfordert keine Änderungen an der vorhandenen Hardware oder Backend-Software. Das Access Gateway kann zusammen mit anderen Netzwerkprodukten, wie z. B. SLBs, Cache-Engines, Firewalls, Routern und drahtlosen IEEE 802.11-Geräten eingesetzt werden.

Citrix empfiehlt, das Access Gateway in der demilitarisierten Zone (DMZ) des Unternehmens zu installieren. Wenn es in der DMZ installiert wird, kann das Access Gateway an zwei Netzwerken teilnehmen: einem privaten Netzwerk und einem öffentlichen Netzwerk mit einer IP-Adresse, die öffentlich geroutet werden kann. Üblicherweise ist das private Netzwerk das Firmennetzwerk und beim öffentlichen handelt es sich um das Internet. Sie können mit dem Access Gateway auch lokale Netzwerke innerhalb der Organisation unterteilen, um den Zugriff zu steuern und die Sicherheit zu erhöhen. Sie können Partitionen zwischen Kabel- oder drahtlosen Netzwerken und Daten- und Sprachnetzwerken erstellen.

Vorbereitung der Installation des Access Gateways

Überprüfen Sie vor dem Installieren des Access Gateways, ob der Inhalt des Kartons mit der Packliste übereinstimmt. Sollte ein auf der Packliste genannter Gegenstand im Karton fehlen, wenden Sie sich an Citrix Customer Care.

Wenn Sie das Access Gateway in einem Rack installieren, finden Sie eine Anleitung dafür im Handbuch *Installationsübersicht für Citrix Access Gateway Standard Edition*.

Für die Installation erforderliches Zubehör und Informationen

Besorgen Sie vor dem Installieren des Access Gateways alles, was für die Erstkonfiguration und den Anschluss an Ihr Netzwerk nötig ist.

Verwenden Sie für die *Erstkonfiguration* **eines** der folgenden Setups:

- Ein Kreuzkabel und einen Windows-Computer
- Zwei Netzwerkkabel, einen Netzwerkswitch und einen Windows-Computer
- Ein serielles Kabel und einen Computer mit Terminalemulationssoftware

Für den Anschluss an ein LAN benötigen Sie Folgendes:

- Ein Netzwerkkabel zum Anschluss des Access Gateways innerhalb einer Firewall oder an einen SLB
- Zwei Netzwerkkabel zum Anschluss des in der demilitarisierten Zone (DMZ) befindlichen Access Gateways an das Internet und das private Netzwerk

Citrix empfiehlt, dass Sie mit der *Access Gateway Standard Edition Pre-Installation Checklist* die folgenden Netzwerkinformationen für die Geräte zusammenstellen:

- Interne IP-Adresse des Access Gateways und zugehörige Subnetzmaske
- Externe IP-Adresse des Access Gateways und zugehörige Subnetzmaske
- Vollqualifizierten Domänennamen des Access Gateways für Netzwerkadressübersetzung (NAT, Network Address Translation)
- IP-Adresse des Standardgatewaygeräts
- Für die Verbindungen zu verwendender Port

Beim Anschluss des Access Gateways an einen Server Load Balancer (SLB) benötigen Sie folgende Informationen:

- IP-Adresse des Access Gateways und zugehörige Subnetzmaske.
- Einstellungen des Server Load Balancers als Standardgatewaygerät (falls erforderlich). Weitere Informationen finden Sie in der Dokumentation des Load Balancer-Herstellers.
- Vollqualifizierten Domänennamen des Server Load Balancers, der als externe öffentliche Adresse des Access Gateways verwendet wird.
- Für die Verbindungen zu verwendender Port.

Hinweis: Das Access Gateway funktioniert nicht mit DHCP (Dynamic Host Configuration Protocol). Für das Access Gateway ist die Verwendung statischer IP-Adressen erforderlich.

Einrichten der Access Gateway-Hardware

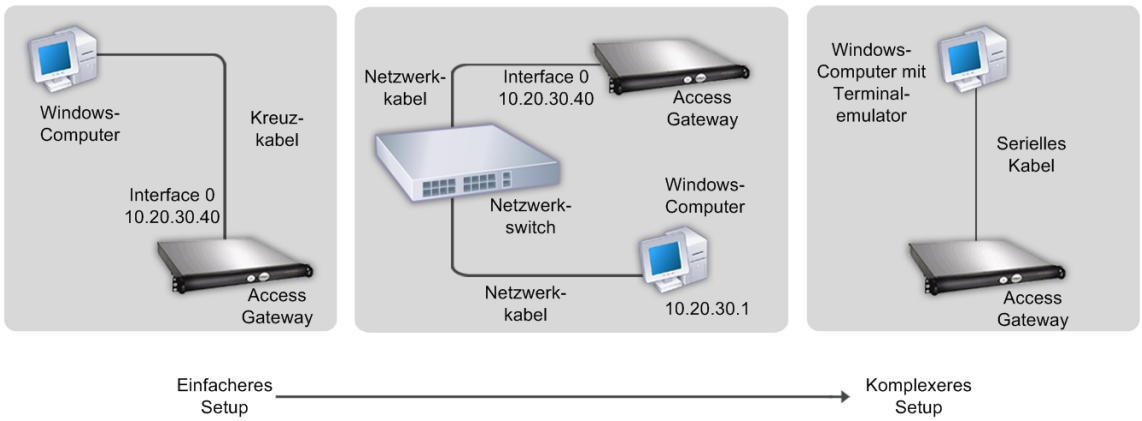
Dieser Abschnitt enthält Anweisungen für die erstmalige Einrichtung des Access Gateways.

So schließen Sie das Access Gateway an:

1. Installieren Sie das Access Gateway in einem Rack, sofern gewünscht.

   Weitere Informationen zum Installieren des Access Gateways in einem Rack finden Sie im Handbuch *Installationsübersicht für Citrix Access Gateway Standard Edition*.

2. Stecken Sie das Stromkabel in die Netzsteckdose.
3. Verbinden Sie entweder das serielle Kabel mit einem Windows-Computer, ein Kreuzkabel mit einem Windows-Computer oder ein RJ45-Netzwerkkabel mit einem Netzwerkswitch und dem Access Gateway.
4. Konfigurieren Sie die TCP/IP-Einstellungen mit der Anleitung unter „Konfigurieren der TCP/IP-Einstellungen für das Access Gateway“ auf Seite 42.



Anschlussmöglichkeiten für das Access Gateway über ein Kreuzkabel, einen Netzwerkswitch oder Terminalemulator

Konfigurieren der TCP/IP-Einstellungen für das Access Gateway

Die vorkonfigurierte IP-Adresse des Access Gateways lautet 10.20.30.40. Die IP-Adresse kann mit einem seriellen Kabel und einem Terminalemulationsprogramm oder durch Anschließen des Access Gateways mit Netzwerkkabeln und dem Administration Tool geändert werden.

Konfigurieren der TCP/IP-Einstellungen mit dem seriellen Kabel

Sie können die serielle Konsole verwenden, um die IP-Adresse und die Subnetzmaske der Access Gateway-Schnittstelle 0 sowie die IP-Adresse des Standardgatewaygeräts festzulegen. Für alle anderen Konfigurationsschritte steht Ihnen das Administration Tool zur Verfügung. Sie können die serielle Konsole auch verwenden, um mit dem Befehl **ping** eine Verbindung zu testen. Wenn Sie das Access Gateway über die serielle Konsole erreichen möchten, bevor Sie irgendwelche Konfigurationseinstellungen vornehmen, schließen Sie das Access Gateway über ein serielles Kabel an einen Computer an, auf dem ein Terminalemulator installiert ist.

Mit der seriellen Konsole haben Sie folgende Optionen für die Konfiguration des Access Gateways:

- **[0] Express Setup:** Konfiguriert die TCP/IP-Einstellungen für Interface 0 auf der Registerkarte **Access Gateway Cluster > General Networking**.
- **[1] Ping:** Hiermit werden andere Netzwerke angesprochen, um die Konnektivität zu überprüfen.
- **[2] Link Modes:** Hiermit werden Duplexmodus und Geschwindigkeitsmodus für Interface 0 auf der Registerkarte **Access Gateway Cluster > General Networking** eingestellt.
- **[3] External Administration Port:**: Hiermit werden Verbindungen zum Administration Tool von einem Remotecomputer aktiviert oder deaktiviert.
- **[4] Display Log:** Zeigt das Access Gateway-Protokoll an.
- **[5] Reset Certificate:** Stellt das in Access Gateway enthaltene Standardzertifikat wieder her.
- **[6] Change Administrative Password:** Hiermit können Sie das Standardadministratorkennwort **rootadmin** ändern.

Wichtig: Citrix empfiehlt, dass Sie das Administratorkennwort ändern, bevor Sie das Access Gateway an Ihr Netzwerk anschließen. Das neue Kennwort kann bis zu 127 Zeichen enthalten und darf nicht mit einem Leerzeichen beginnen oder enden.

- **[7] Help:** Zeigt Hilfeinformationen an.
- **[8] Log Out:** Meldet Sie vom Access Gateway ab.

Hinweis: Citrix empfiehlt, beide Netzwerkadapter des Geräts zu verwenden. Nach der Konfiguration der TCP/IP-Einstellungen für Interface 0 konfigurieren Sie die TCP/IP-Einstellungen für Interface 1 mit dem Administration Tool.

So konfigurieren Sie TCP/IP-Einstellungen mit einem seriellen Kabel:

1. Verbinden Sie das serielle Kabel mit der neunpoligen seriellen Schnittstelle am Access Gateway und schließen Sie das andere Ende an einen Computer an, auf dem ein Terminalemulator installiert ist.
2. Starten Sie den Terminalemulator auf dem Computer, z. B. HyperTerminal.

Hinweis: HyperTerminal ist nicht automatisch unter Windows 2000 Server oder Windows Server 2003 installiert. Installieren Sie HyperTerminal über die Option **Software** in der Systemsteuerung.

---

3. Legen Sie für die serielle Verbindung 9600 Bit/s, 8 Datenbits, keine Parität und 1 Stoppbit fest. Optional kann die Hardware-Flusssteuerung aktiviert werden.
4. Schalten Sie das Access Gateway ein. Nach etwa drei Minuten wird auf dem Computerterminal die serielle Konsole angezeigt.
5. Wenn Sie HyperTerminal verwenden, drücken Sie nun die **Eingabetaste**.
6. Geben Sie an der seriellen Konsole die Standardanmeldeinformationen für den Administrator ein. Der Benutzername lautet **root** und das Kennwort ist **rootadmin**.

Wichtig: Citrix empfiehlt, das Administratorkennwort zu ändern. Sie können hierzu das Administration Portal oder die serielle Konsole verwenden.

---

7. Geben Sie zum Festlegen der IP-Adresse, der Subnetzmaske und des Standardgatewaygeräts für die Schnittstelle 0 **0** ein und drücken Sie dann die **Eingabetaste**, um das Express Setup zu starten. Die an den einzelnen Eingabeaufforderungen eingegebenen Informationen werden angezeigt. Geben Sie zum Bestätigen Ihrer Änderungen **y** ein. Das Access Gateway wird neu gestartet.
8. Um zu überprüfen, ob das Access Gateway ein angeschlossenes Netzwerkgerät pingen kann, geben Sie **1** und die IP-Adresse des Geräts ein.
9. Ziehen Sie das serielle Kabel ab und schließen Sie das Access Gateway entweder mit einem Kreuzkabel an einen Windows-Computer oder mit einem Netzwerkkabel an einen Netzwerkswitch an. Schalten Sie dann das Access Gateway ein.

Zusätzliche Access Gateway-Einstellungen werden mit dem Administration Tool konfiguriert.

Konfigurieren der TCP/IP-Einstellungen mit Netzwerkkabeln

Das Access Gateway hat zwei Netzwerkadapter. Ein Netzwerkadapter kommuniziert mit dem Internet und den Clientcomputern, die sich außerhalb des Unternehmensnetzwerks befinden. Der andere Netzwerkadapter übernimmt die Kommunikation innerhalb des internen Netzwerks.

Citrix empfiehlt, beide Netzwerkadapter mit maximaler Sicherheit zu konfigurieren. Wenn nur ein Netzwerkadapter verwendet wird, muss dieser mit NAT (Network Address Translation) für interne Ressourcen geroutet werden können. Außerdem wird bei Verwendung nur eines Netzwerkadapters der Datendurchsatz des Netzwerks halbiert, was zu Engpässen bei der Datenübertragung führen kann.

Für die Installation des Access Gateways und die Konfiguration der TCP/IP-Einstellungen können Sie Netzwerkkabel verwenden, z. B. RJ45-Netzwerkkabel oder Kreuzkabel. Die RJ45-Kabel werden zum Verbinden von Netzwerkswitch und Access Gateway verwendet. Mit den Kreuzkabeln werden Windows-Computer und Access Gateway verbunden.

So konfigurieren Sie die TCP/IP-Einstellungen mit Netzwerkkabeln:

1. Schalten Sie das Access Gateway ein.

   Nach etwa drei Minuten ist das Access Gateway für die Erstkonfiguration in Ihrem Netzwerk bereit.

2. Öffnen Sie einen Webbrowser und geben Sie https://10.20.30.40:9001 ein, um das Administration Portal zu öffnen. Verwenden Sie den Standardbenutzernamen **root** und das zugehörige Kennwort **rootadmin**.

3. Klicken Sie auf der Registerkarte **Downloads** unter **Access Gateway Administration Tool** auf **Install the Access Gateway Administration Tool**.

   Folgen Sie den Anweisungen, um die Installation abzuschließen.

4. Melden Sie am Administration Tool mit dem Standardbenutzernamen und dazugehörigem Kennwort an.

5. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.

6. Geben Sie auf der Registerkarte **General Networking** unter **Interface 0** und **Interface 1** in den Feldern **IP address** die neuen IP-Adressen des Geräts ein.

   Citrix empfiehlt, die Option **Use both interfaces** (Beide Schnittstellen verwenden) zu aktivieren.

7. Geben Sie in den Feldern **Subnet mask** die entsprechenden Subnetzmasken für die für die Schnittstelle(n) eingegebenen IP-Adressen ein.
8. Geben Sie unter **External FQDN** den vollqualifizierten Domänennamen ein.

Wichtig: Der vollqualifizierte Domänenname muss dem Namen entsprechen, der auf dem digitalen Zertifikat und der Lizenz für das Access Gateway angegeben ist.

---

9. Wählen Sie unter **Duplex mode** die gewünschte Datenübertragungsrichtung aus.

   Die Standardeinstellung lautet **Auto**. Sie können außerdem noch **Full Duplex** oder **Half Duplex** auswählen.
10. Wählen Sie unter **Speed Mode** die Netzwerkgeschwindigkeit des Adapters aus.

    Die Standardeinstellung lautet **Auto**. Sie können auch **10 Mbps**, **100 Mbps** oder **1000 Mbps** auswählen.
11. Geben Sie unter **Maximum transmission unit (MTU)** die Übertragungseinheit an, die die maximale Größe des übertragenen Pakets festlegt.

    Der Standardwert ist 1500.
12. Geben Sie unter **Port** den Port an, der für eingehende Verbindungen verwendet werden soll. Der Standardwert ist 443.
13. Wenn Sie ein Standardgateway konfigurieren möchten, geben Sie im Bereich **Default Gateway** unter **IP address** die IP-Adresse des Gateways ein. Wählen Sie unter **Interface** den Netzwerkadapter auf dem Access Gateway aus, mit dem das Standardgateway kommuniziert.

    Dies ist, abhängig von Ihrer Netzwerkkonfiguration, die IP-Adresse des Standardgatewaygeräts, wie z. B. des Hauptrouters, der Firewall oder des SLB. Diese IP-Adresse muss mit der Standardgatewayeinstellung auf den Computern im selben Subnetz übereinstimmen.

    Informationen zum Zusammenhang zwischen dem Standardgateway und dem dynamischen oder statischen Routing finden Sie unter „Konfigurieren weiterer Netzwerkeinstellungen“ auf Seite 62.

Nachdem Sie die Netzwerkeinstellungen auf dem Access Gateway konfiguriert haben, müssen Sie das Gerät neu starten.

Hinweis: Ein Neustart des Access Gateways ist erst notwendig, wenn Sie alle Konfigurationsschritte vollständig ausgeführt haben. Hierzu gehören die Konfiguration des Netzwerkzugriffs für das Gerät sowie das Installieren von Zertifikaten und Lizenzen. Weitere Informationen über die Konfiguration zusätzlicher Netzwerkeinstellungen finden Sie unter „Konfigurieren des Access Gateways für die Netzwerkumgebung“ auf Seite 49.

Umleiten von Verbindungen auf Port 80 an einen sicheren Port

Standardmäßig lässt das Access Gateway keine unsicheren Verbindungen auf Port 80 zu. Wenn ein Benutzer versucht, mit HTTP auf Port 80 eine Verbindung zum Access Gateway herzustellen, kommt die Verbindung nicht zustande.

Sie können das Access Gateway so konfigurieren, dass HTTP-Verbindungsversuche auf Port 80 automatisch an sichere Verbindungen auf Port 443 (oder einem anderen sicheren Port) umgeleitet werden.

Wenn ein Benutzer versucht, eine unsichere Verbindung auf Port 80 herzustellen, konvertiert das Access Gateway diesen Verbindungsversuch automatisch in eine sichere (mit SSL verschlüsselte) Verbindung auf Port 443.

So leiten Sie unsichere Verbindungen um:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf die Registerkarte **General Networking**.
3. Klicken Sie auf die Schaltfläche **Advanced**.
4. Aktivieren Sie die Option **Redirect any requests for port 80 to a secure port**.
5. Klicken Sie auf **OK**.

Hinweis: Wenn Sie die Standardeinstellung **Do not accept connections on port 80** verwenden, schlagen alle Verbindungsversuche auf Port 80 fehl und es wird nicht versucht, sie an Port 443 umzuleiten.

Konfigurieren der TCP/IP-Einstellungen für eine Double-Hop-Bereitstellung

Das Access Gateway kann in einer Double-Hop-DMZ installiert werden, um Zugriff auf eine Serverfarm zu geben. Weitere Informationen über diese Art der Bereitstellung finden Sie unter „Bereitstellen des Access Gateways in einer Double-Hop-DMZ“ auf Seite 223.

Neustarten des Access Gateways

Starten Sie das Access Gateway nach der Konfiguration der Netzwerkeinstellungen neu.

So starten Sie das Access Gateway neu:

1. Klicken Sie im Administration Tool auf die Registerkarte **Access Gateway Cluster** und öffnen Sie das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** neben **Restart the appliance** auf **Restart**.

   - oder -

   Klicken Sie im Menü **Action** auf **Restart** *Name des Geräts*, wobei *Name des Geräts* der Name des Access Gateways ist.

Sie können das Access Gateway auch über das Administration Portal neu starten.

So starten Sie das Access Gateway über das Administration Portal neu:

Klicken Sie im Administration Portal auf **Maintenance**. Klicken Sie neben **Restart the Server** auf **Restart**.

Konfigurieren des Access Gateways für die Netzwerkumgebung

Sobald Sie die grundlegenden TCP/IP-Einstellungen auf dem Access Gateway festgelegt haben, konfigurieren Sie das Gerät für Ihre Netzwerkumgebung. Die weitere Konfiguration des Access Gateways umfasst die folgenden Schritte:

- Installieren von Lizenzen
- Erstellen und Installieren von Zertifikaten
- Konfigurieren weiterer Netzwerkeinstellungen
- Konfigurieren von Datum und Uhrzeit auf dem Access Gateway
- Verwenden der Standardportalseite

Installieren von Lizenzen

Die Access Gateway-Lizenzüberwachung begrenzt die Anzahl der gleichzeitigen Benutzersitzungen auf die Anzahl der gekauften Lizenzen. Wenn Sie also 100 Lizenzen kaufen, können 100 gleichzeitige Sitzungen stattfinden. Sobald ein Benutzer eine Sitzung beendet, wird diese Lizenz für den nächsten Benutzer freigegeben. Wenn sich ein Benutzer von mehreren Computern aus am Access Gateway anmeldet, benötigt er für jede Sitzung eine eigene Lizenz.

Wenn alle Lizenzen in Gebrauch sind, können so lange keine weiteren Verbindungen mehr geöffnet werden, bis ein Benutzer eine Sitzung beendet oder der Administrator mit dem Real-time Monitor eine der Verbindungen schließt und damit eine Lizenz freigibt. Informationen zur Verwendung des Real-time Monitors zum Schließen von Verbindungen finden Sie unter „Konfigurieren von Benutzerverbindungen für den Secure Access Client“ auf Seite 139.

Lizenzen für das Access Gateway werden mit dem Administration Tool installiert. Lizenzdateien werden auf der Basis des Hostnamens erstellt, wobei der vollqualifizierte Domänenname des Access Gateways verwendet wird. Das Access Gateway, auf dem die Lizenzen installiert sind (auch als *Lizenzserver* bezeichnet), verarbeitet die installierten Lizenzdateien; ungültige Lizenzdateien werden nicht berücksichtigt.

Befinden sich mehrere Access Gateway-Geräte im Netzwerk, fungiert ein Access Gateway als Lizenzserver, der den anderen Geräten die Lizenzen zuweist. Sobald ein Benutzer sich an einem anderen Gerät im Netzwerk anmeldet, wird die Lizenz von dem Access Gateway abgerufen, das als Lizenzserver arbeitet. In einem Cluster werden die installierten Lizenzen nicht auf den anderen Geräten veröffentlicht. Weitere Informationen zur Verwendung von Lizenzen mit mehreren Geräten finden Sie unter „Konfigurieren von Lizenzen für mehrere Geräte“ auf Seite 52.

Wichtig: Der Hostname in der Lizenzdatei muss genau (inklusive Groß- und Kleinschreibung) mit dem Hostnamen auf dem Access Gateway übereinstimmen.

Wenn Sie Access Gateway Advanced Edition verwenden, wird die Lizenzierung vom Citrix Lizenzserver übernommen. Weitere Informationen zur Lizenzierung von Access Gateway Advanced Edition finden Sie im *Citrix Access Suite-Lizenzierungshandbuch* und im *Administratorhandbuch für Access Gateway Advanced Edition*.

Abrufen der Lizenzdateien

Nach erfolgter Installation des Access Gateways können Sie Ihre Lizenzdateien von Citrix abrufen. Rufen Sie hierzu die Website http://www.mycitrix.com/ auf, greifen Sie dort auf Ihre verfügbaren Lizenzen zu und erstellen Sie eine Lizenzdatei. Laden Sie die erstellte Lizenzdatei auf den Computer herunter, auf dem das Administration Tool installiert ist. Anschließend können Sie die Lizenzdatei auf das Access Gateway hochladen.

Halten Sie beim Aufrufen der Citrix Website die folgenden Angaben bereit:

Lizenzcode: Den Code finden Sie auf der Access Gateway-CD, in der E-Mail von Citrix oder im Subscription Advantage Management-Renewal-Informationssystem (SAMRI).

Benutzer-ID und Kennwort für MyCitrix: Sie können sich auf MyCitrix für dieses Kennwort registrieren.

Hinweis: Wenn Sie diese Informationen nicht haben, wenden Sie sich bitte an Citrix Customer Care.

Vollqualifizierter Domänenname des Access Gateways: Bei der Eingabe dieses Namens auf MyCitrix wird zwischen Groß- und Kleinschreibung unterschieden. Tragen Sie den vollqualifizierten Domänennamen daher exakt so ein, wie er auf der Registerkarte **Access Gateway Cluster > General Networking** aufgeführt ist.

Anzahl der Lizenzen, die in die Lizenzdatei aufgenommen werden sollen: Sie müssen nicht alle Lizenzen, auf die Sie Anspruch haben, gleichzeitig downloaden. Wenn Ihr Unternehmen beispielsweise 100 Lizenzen erworben hat, können Sie zunächst 50 Lizenzen herunterladen und die verbleibenden Lizenzen dann zu einem späteren Zeitpunkt in einer anderen Lizenzdatei herunterladen. Auf dem Access Gateway können mehrere Lizenzdateien installiert werden.

So rufen Sie die Lizenzdatei ab:

1. Gehen Sie in einem Webbrowser zu http://www.mycitrix.com/.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

   Bei der ersten Anmeldung an der Website werden Sie aufgefordert, weitere Informationen anzugeben.
3. Klicken Sie auf **Meine Tools > Activation System/Lizenzen verwalten > Erwerbungen anzeigen > Zum Zuweisen klicken**.
4. Folgen Sie den Anweisungen, um Ihre Lizenzdatei abzurufen.

Nachdem der Download der Lizenzdatei auf Ihren Computer erfolgreich abgeschlossen wurde, können Sie die Datei auf dem Access Gateway installieren.

So installieren Sie eine Lizenz auf dem Access Gateway-Gerät:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf die Registerkarte **Licensing**.
3. Wählen Sie **Use this appliance as the license server**.
4. Klicken Sie neben **Install a license file** auf **Browse**, navigieren Sie zur Lizenzdatei und klicken Sie auf **Öffnen**.

5. Sobald die Lizenzdatei auf das Access Gateway hochgeladen ist, klicken Sie auf **Submit**.

Wichtig: Citrix empfiehlt, von allen Lizenzdateien, die Sie erhalten, jeweils eine Kopie auf dem lokalen Computer zu speichern. Wenn Sie eine Sicherungskopie der Konfigurationsdatei speichern, werden alle hochgeladenen Lizenzdateien in die Sicherung übernommen. Wenn die Access Gateway-Serversoftware neu installiert werden muss und Sie nicht auf eine Sicherungskopie der Konfiguration zurückgreifen können, benötigen Sie die Original-Lizenzdateien.

Konfigurieren von Lizenzen für mehrere Geräte

Wenn Sie mehrere Geräte installiert haben, legen Sie ein Access Gateway fest, das als Lizenzserver fungieren soll. Installieren Sie alle Lizenzen auf einem Access Gateway, das dadurch zum Lizenzserver wird. Die anderen Geräte rufen die Lizenzen von diesem Access Gateway ab. Die anderen Geräte im Netzwerk können auch dann eine Verbindung zum Lizenzserver herstellen und Lizenzen abrufen, wenn sie nicht zum Cluster gehören. Die Lizenzen werden den Geräten unabhängig von ihrem jeweiligen Status im Netzwerk zugewiesen.

So rufen Sie Lizenzen vom Lizenzserver ab:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway, das nicht als Lizenzserver fungiert.
2. Klicken Sie auf die Registerkarte **Licensing**.
3. Wählen Sie **Use a different appliance as the license server**.
4. Geben Sie in das Feld **FQDN or IP address** den vollqualifizierten Domänennamen oder die IP-Adresse des Lizenzservers ein.
5. Ändern Sie die Portnummern in den Feldern **Manager port** und **Vendor port** oder übernehmen Sie die Standardeinstellungen 27000 und 27001.
6. Klicken Sie auf **Submit**.
7. Wiederholen Sie dieses Verfahren für alle Access Gateway-Geräte im Cluster, die keine Lizenzserver sind.

Der Manager-Port stellt den ersten Kontakt zum Remote-Access Gateway her und leitet die Verbindung an den Lizenzserver weiter. Anschließend wird die Kommunikation vom Manager-Port an den Vendor-Port übergeben. Der Vendor-Port wird auf dem Lizenzserver ausgeführt und erteilt die Lizenz über die Portnummer 27001. Die Portnummern lassen sich an die vorliegende Firewall-Konfiguration anpassen. Der Manager-Port zeichnet die ausgecheckten Lizenzen und die Access Gateway-Geräte, auf denen diese Lizenzen verwendet werden, auf.

Unter Umständen müssen Sie neue Firewall-Regeln anlegen, damit der Netzwerkzugriff auf die Lizenzserverports möglich wird.

Informationen zu Lizenzen

Auf der Registerkarte **Licensing** finden Sie Informationen zu den Lizenzen, die auf dem Access Gateway installiert sind: Unter anderem:

- Gesamtanzahl der verfügbaren Lizenzen
- Anzahl der derzeit verwendeten Lizenzen
- Subscription Advantage-Enddatum
- Ausgabedatum der Lizenzen
- Ablaufdatum der Lizenzen
- Seriennummer der Lizenzen
- Art der Lizenzen

Falls zwei Lizenzen mit derselben Seriennummer installiert sind, werden diese Dateien nicht einzeln gerechnet. Das Gerät, das als Lizenzserver fungiert, wählt eine der Lizenzdateien aus und weist den Benutzern die entsprechenden Lizenzen zu.

Darüber hinaus können Sie Lizenzprotokolle mit ausführlichen Informationen zur Lizenznutzung finden. Die Protokolle befinden sich nach dem Herunterladen in einer komprimierten Datei mit der Bezeichnung license_logs.zip.

So laden Sie Lizenzprotokolle herunter:

1. Klicken Sie auf der Registerkarte **Access Gateway Cluster** auf die Registerkarte **Licensing**.
2. Klicken Sie unter **Information about this Access Gateway** neben **Download licensing logs** auf **Download All**.
3. Legen Sie den Ordner fest, in den die Dateien heruntergeladen werden sollen, und klicken Sie auf **Speichern**.

Wenn Sie Änderungen an der Lizenzierung auf dem Access Gateway vornehmen, können Sie die Angaben auf der Registerkarte **Licensing** aktualisieren.

So aktualisieren Sie die Lizenzierungsinformationen:

Klicken Sie unter **Information about the licensing server** auf **Refresh all information**.

Aktualisieren vorhandener Lizenzen

Als Subscription Advantage-Mitglied können Sie Ihre vorhandenen Access Gateway-Lizenzen austauschen (migrieren) und damit Ihre Lizenzdateien auf den neuesten Stand bringen.

Kulanzzeitraum für die Lizenzierung

Bei der Installation des Access Gateways beginnt ein viertägiger Kulanzzeitraum, während dessen Ihnen zwei Lizenzen zur Verfügung stehen. Bis zum Ablauf dieser Frist muss die Lizenz auf dem Gerät installiert werden, ansonsten können sich die Benutzer nicht anmelden.

Sollte der Access Gateway-Lizenzserver ausfallen, beginnt ein dreißigtägiger Kulanzzeitraum auf dem Remotegerät. Das Remote-Access Gateway speichert das Datum, an dem zum letzten Mal eine Verbindung zum Lizenzserver aufgenommen wurde. Die Benutzer können sich während dieses Kulanzzeitraums wie gewohnt anmelden. Sobald das Remotegerät den Lizenzserver erkennt, wird der dreißigtägige Kulanzzeitraum zurückgesetzt. Bei einem erneuten Ausfall des Lizenzservers erhalten die Benutzer erneut eine dreißigtägigen Kulanzzeitraum.

Testen der Lizenzinstallation

Erstellen Sie zum Testen der Konfiguration einen Testbenutzer und melden Sie sich dann mit den Anmeldeinformationen, die Sie für diesen Benutzer angelegt haben, über den Secure Access Client an.

So testen Sie die Konfiguration:

1. Öffnen Sie das Administration Tool.
2. Klicken Sie auf die Registerkarte **Access Policy Manager**.
3. Klicken Sie mit der rechten Maustaste im linken Bereich auf den Ordner **Local Users** und klicken Sie dann auf **New User**.
4. Geben Sie im Dialogfeld **New User** in das Feld **User Name** einen Benutzernamen ein und in das Feld **Password** entsprechend das Kennwort. Wiederholen Sie die Eingabe des Kennworts im Feld **Verify Password** und klicken Sie auf **OK**.

5. Geben Sie in einem Webbrowser die Adresse des Access Gateways ein (wahlweise die IP-Adresse oder den vollqualifizierten Domänennamen) und stellen Sie so eine Verbindung zum internen oder externen Interface her. Die Syntax lautet dabei *https://IP-Adresse* bzw. *https://vollqualifizierter Domänenname*.
6. Geben Sie die Anmeldeinformationen ein. Das **Citrix Access Gateway Portal** wird geöffnet.
7. Klicken Sie auf **Eigener Computer** und dann auf **Verbinden**.

   Das Secure Access Client-Verbindungssymbol wird im Infobereich angezeigt; dies zeigt an, dass die Verbindung erfolgreich hergestellt wurde.

Die Erstkonfiguration ist damit abgeschlossen. Nach der Erstkonfiguration können Sie die zugänglichen Netzwerke konfigurieren, sodass Verbindungen zu allen Netzwerkressourcen (z. B. E-Mail, Webserver, Dateifreigaben) auf dieselbe Weise wie an Ihrem Arbeitsplatz möglich sind. Versuchen Sie zum Testen der Konfiguration, eine Verbindung zu Anwendungen und Ressourcen im Unternehmensnetzwerk herzustellen.

Erstellen und Installieren von Zertifikaten

Das Access Gateway enthält ein digitales Zertifikat, das nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert ist. Installieren Sie auf dem Access Gateway ein digitales X.509-Zertifikat, das zu Ihrem Unternehmen gehört und von einer Zertifizierungsstelle signiert wurde. Ihr Unternehmen kann als seine eigene Zertifizierungsstelle agieren, Sie können aber auch ein digitales Zertifikat von einer gewerblichen Zertifizierungsstelle beziehen, wie z. B. Verisign und Thawte.

Achtung: Das Betreiben des Access Gateways ohne ein von einer Zertifizierungsstelle signiertes digitales Zertifikat kann VPN-Verbindungen der Gefahr böswilliger Angriffe aussetzen.

Das Access Gateway akzeptiert Zertifikatdateien im PEM-Format (Privacy Enhanced Mail). PEM ist ein Textformat, das die Base-64-Verschlüsselung des binären DER-Formats (Distinguished Encoding Rules) darstellt. Das PEM-Format legt die Verwendung der Text-BEGIN- und -END-Zeilen fest, die die Art des verschlüsselten Inhalts angeben.

Es gibt zwei Möglichkeiten, ein sicheres Zertifikat und einen privaten Schlüssel auf dem Access Gateway zu installieren:

- Erstellen Sie mit dem Administration Tool eine Zertifikatsignieranforderung (Certificate Signing Request, CSR). Daraufhin werden ein Zertifikat und ein privater Schlüssel erstellt. Der private Schlüssel verbleibt auf dem Access Gateway, während das Zertifikat zum Signieren an die Zertifizierungsstelle gesendet wird. Nachdem das Zertifikat zurückgesendet wurde, wird es auf dem Gerät installiert. Während der Installation wird das Zertifikat mit dem kennwortgeschützten privaten Schlüssel zusammengeführt. Citrix empfiehlt, dieses Verfahren zum Erstellen und Installieren sicherer Zertifikate zu verwenden.
- Installieren Sie ein PEM-Zertifikat und einen privaten Schlüssel von einem Windows-Computer aus. Bei diesem Verfahren werden ein signiertes Zertifikat und ein privater Schlüssel gemeinsam hochgeladen. Das Zertifikat wird von einer Zertifizierungsstelle signiert und dann mit dem privaten Schlüssel zusammengeführt.

Übersicht über Zertifikatsignieranforderungen

Bevor Sie ein Zertifikat auf das Access Gateway hochladen können, müssen Sie eine CSR (Certificate Signing Request, Zertifikatsignieranforderung) und einen privaten Schlüssel generieren. Die CSR wird mit dem im Administration Tool enthaltenen Certificate Request Generator erstellt. Der Certificate Request Generator ist ein Assistent zum Erstellen einer CSR-Datei. Die erstellte Datei wird per E-Mail zum Signieren an die Zertifizierungsstelle gesendet. Die Zertifizierungsstelle signiert das Zertifikat und sendet es an die angegebene E-Mail-Adresse zurück. Anschließend können Sie das Zertifikat auf dem Access Gateway installieren.

Zur sicheren Datenübertragung mit SSL/TLS muss ein Serverzertifikat auf dem Access Gateway vorliegen. So können Sie ein Serverzertifikat abrufen und auf dem Access Gateway installieren:

- Erstellen Sie mit dem Certificate Request Generator eine CSR (myreq.csr) und einen privaten Schlüssel (private.key). Informationen hierzu finden Sie unter „Erstellen einer Zertifikatsignieranforderung“ auf Seite 57.
- Senden Sie die Datei myreq.csr per E-Mail an einen autorisierten Zertifikatsanbieter.
- Sobald Sie die signierte Zertifikatdatei von der Zertifizierungsstelle erhalten, laden Sie das Zertifikat mit dem Administration Tool hoch. Das Administration Tool wandelt das Zertifikat automatisch in das vom Access Gateway geforderte PEM-Format um.

Kennwortgeschützte private Schlüssel

Die mit der Zertifikatsignieranforderung erstellten privaten Schlüssel werden verschlüsselt und kennwortgeschützt auf dem Access Gateway gespeichert. Beim Erstellen der Zertifikatsignieranforderung werden Sie aufgefordert, ein Kennwort für den privaten Schlüssel festzulegen. Dieses Kennwort schützt den privaten Schlüssel vor Manipulationen und ist außerdem beim Wiederherstellen einer gespeicherten Konfiguration auf dem Access Gateway erforderlich. Kennwörter werden in jedem Fall verwendet, unabhängig davon, ob der private Schlüssel verschlüsselt ist.

Wenn Sie ein Upgrade auf Version 4.5 durchführen und die Konfigurationsdatei speichern, kann diese Datei auf früheren Versionen des Access Gateways nicht mehr verwendet werden. Wenn Sie versuchen, die Konfigurationsdatei aus Version 4.5 auf eine frühere Version hochzuladen, kann das Access Gateway nicht mehr verwendet werden.

Darüber hinaus können Sie eine kennwortgeschützte Gruppe aus Zertifikat und privatem Schlüssel im PKCS12-Format importieren. Auf diese Weise lassen sich verschlüsselte und kennwortgeschützte private Schlüssel und Zertifikate importieren, die auf dem Access Gateway erstellt wurden.

Achtung: Wenn Sie die Konfiguration unter Version 4.5 des Access Gateways speichern, installieren Sie diese Konfiguration nicht auf früheren Versionen des Geräts. Der Grund hierfür ist, dass der private Schlüssel in Version 4.5 verschlüsselt ist und ältere Versionen ihn nicht entschlüsseln können. Dadurch wird das Gerät funktionsuntüchtig.

Erstellen einer Zertifikatsignieranforderung

Die Zertifikatsignieranforderung wird mit dem im Administration Tool enthaltenen Certificate Request Generator erstellt.

So erstellen Sie eine Zertifikatsignieranforderung:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Geben Sie auf der Registerkarte **Certificate Signing Request** die erforderlichen Informationen ein und klicken Sie dann auf **Generate Request**.

Hinweis: Geben Sie in das Feld **Access Gateway FQDN** den vollqualifizierten Domänennamen ein, der auf der Registerkarte **General Networking** aufgeführt ist. Geben Sie unter **Password** das Kennwort für den privaten Schlüssel ein.

---

3. Es wird eine CSR-Datei erstellt. Speichern Sie die CSR-Datei auf dem lokalen Computer.
4. Senden Sie das Zertifikat per E-Mail an die Zertifizierungsstelle.

   Der Zertifikatsanbieter sendet Ihnen per E-Mail ein signiertes Zertifikat zurück. Installieren Sie dieses signierte Zertifikat auf dem Access Gateway.

Hinweis: Beim Speichern der Access Gateway-Konfiguration werden auch alle bereits installierten Zertifikate mit gesichert.

Nachdem Sie die Zertifikatsanforderung an die Zertifizierungsstelle gesendet haben, führen Sie die nachfolgenden Aufgaben auf dem Access Gateway erst dann wieder aus, wenn Sie das signierte Zertifikat auf dem Gerät installiert haben:

- Erstellen einer weiteren Zertifikatsignieranforderung
- Hochladen einer gespeicherten Konfigurationsdatei
- Veröffentlichen von Konfigurationseinstellungen von einem anderen Gerät im Cluster

---

Wichtig: Wenn Sie ein Zertifikat erstellt und an die Zertifizierungsstelle gesendet haben, erstellen Sie keine weitere Zertifikatsignieranforderung. Das Access Gateway kann nur einen privaten Schlüssel speichern. Wird die Zertifikatsignieranforderung erneut ausgeführt, wird der private Schlüssel überschrieben und das signierte Zertifikat findet keinen passenden Schlüssel als Gegenstück.

So installieren Sie eine Zertifikatdatei mit dem Administration Tool:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf der Registerkarte **Administration** neben **Upload a .crt signed certificate** auf **Browse**.

   Diese Schaltfläche kommt nur dann zum Einsatz, wenn Sie ein signiertes Zertifikat installieren, das über die Registerkarte **Certificate Signing Request** erstellt wurde.
3. Suchen Sie die Datei, die hochgeladen werden soll, und klicken Sie auf **Öffnen**.

Sie können das Zertifikat auch über das Administration Portal hochladen.

So installieren Sie ein Zertifikat über das Administration Portal:

1. Klicken Sie auf der **Administration Portal**-Hauptseite auf **Maintenance**.
2. Klicken Sie neben **Upload Signed Certificate (.crt)** auf **Browse**.
3. Navigieren Sie zum Zertifikat und laden Sie die Datei hoch.

Zurücksetzen des Zertifikats auf die Standardversion

Das Access Gateway enthält ein Zertifikat, das keine digitale Signatur einer Zertifizierungsstelle trägt. Für den Fall, dass die Konfiguration des Geräts wiederhergestellt werden muss, können Sie das Zertifikat auf das Standardzertifikat aus dem Lieferumfang des Access Gateways zurücksetzen. Wählen Sie hierzu in der seriellen Konsole die Option zum Zurücksetzen des Zertifikats.

So setzen Sie das Zertifikat auf die Standardversion zurück:

1. Verbinden Sie das serielle Kabel mit der neunpoligen seriellen Schnittstelle am Access Gateway und schließen Sie das andere Ende an einen Computer an, auf dem ein Terminalemulator installiert ist.
2. Starten Sie den Terminalemulator auf dem Computer, z. B. HyperTerminal.

Hinweis: Bei Windows 2000 Server und Windows Server 2003 wird HyperTerminal nicht automatisch installiert. Installieren Sie HyperTerminal über **Software** in der Systemsteuerung installieren.

---

3. Legen Sie für die serielle Verbindung 9600 Bit/s, 8 Datenbits, keine Parität und 1 Stoppbit fest. Optional kann die Hardware-Flusssteuerung aktiviert werden.
4. Schalten Sie das Access Gateway ein. Nach etwa drei Minuten wird auf dem Computerterminal die serielle Konsole angezeigt.
5. Wenn Sie HyperTerminal verwenden, drücken Sie nun die **Eingabetaste**.
6. Um das Zertifikat auf das Standardzertifikat zurückzusetzen, geben Sie **5** ein und drücken Sie die **Eingabetaste**.

Installieren eines Zertifikats und eines privaten Schlüssels von einem Windows-Computer aus

Wenn Sie einen Load Balancer einsetzen oder ein signiertes digitales Zertifikat mit einem privaten Schlüssel besitzen, das auf einem Windows-Computer gespeichert ist, können Sie dieses Zertifikat auf das Access Gateway hochladen. Befindet sich das Access Gateway nicht hinter einem Load Balancer, muss das Zertifikat den vollqualifizierten Domänennamen des Access Gateways aufweisen. Falls das Access Gateway hinter einem Load Balancer bereitgestellt ist, müssen alle Geräte dasselbe Zertifikat und denselben privaten Schlüssel enthalten. Weitere Informationen hierzu finden Sie unter „Konfigurieren mehrerer Geräte für die Verwendung eines Load Balancers“ auf Seite 275.

So installieren Sie ein Zertifikat und einen privaten Schlüssel von einem Windows-Computer aus:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Administration**.
3. Klicken Sie neben **Upload a .pem private key and signed certificate** auf **Browse**.
4. Gehen Sie zum Zertifikat und klicken Sie auf **Öffnen**.

   Beim Hochladen des Zertifikats auf das Access Gateway werden Sie aufgefordert, ein Kennwort festzulegen, mit dem der private Schlüssel verschlüsselt werden soll.

Installieren von Stammzertifikaten auf dem Access Gateway

Die Stammzertifikate werden von der Zertifizierungsstelle ausgestellt. Mit diesen Stammzertifikaten validieren die SSL-Clients die von einem SSL-Server vorgelegten Zertifikate. Wenn ein SSL-Client eine Verbindung zu einem SSL-Server aufbaut, weist der Server ein Zertifikat vor. Der Client schlägt daraufhin im Stammzertifikatspeicher nach, ob das vom SSL-Server vorgelegte Zertifikat von einer Zertifizierungsstelle signiert ist, die für das Stammzertifikat als vertrauenswürdig gilt. Wird das Access Gateway in einer Umgebung bereitgestellt, in der es als Client bei SSL-Handshakes fungiert (also verschlüsselte Verbindungen zu einem anderen Server einleitet), installieren Sie ein vertrauenswürdiges Stammzertifikat auf dem Access Gateway.

Wenn Sie beispielsweise das Access Gateway mit Citrix Presentation Server und mit dem Webinterface installieren, können Sie Verbindungen vom Access Gateway zum Webinterface mit SSL verschlüsseln. Bei dieser Konfiguration muss ein vertrauenswürdiges Stammzertifikat auf dem Access Gateway installiert werden.

Das auf dem Access Gateway installierte Stammzertifikat muss im PEM-Format vorliegen. Unter Windows werden Stammzertifikate im PEM-Format gelegentlich mit der Dateinamenerweiterung .cer gekennzeichnet.

Sollen Zertifikate für interne Verbindungen validiert werden, muss auf dem Access Gateway ein Stammzertifikat installiert sein.

So installieren Sie ein Stammzertifikat auf dem Access Gateway:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf der Registerkarte **Administration** neben **Manage trusted root certificates** auf **Manage**.
3. Klicken Sie auf der Registerkarte **Manage** auf **Upload Trusted Root Certificate**.
4. Navigieren Sie zur Datei und klicken Sie auf **Öffnen**.

Mit **Remove Trusted Root Certificate** können Sie das Stammzertifikat wieder entfernen.

Installieren mehrerer Stammzertifikate

Es ist möglich, mehrere Stammzertifikate auf dem Access Gateway zu installieren; diese Zertifikate müssen sich allerdings in einer einzigen Datei befinden. Beispiel: Sie können eine Textdatei in einem Texteditor (z. B. in Editor) erstellen, die alle Stammzertifikate enthält. Öffnen Sie die einzelnen Stammzertifikate in einer anderen Instanz des Texteditors. Kopieren Sie den Inhalt der Zertifikate und fügen Sie diesen kopierten Inhalt jeweils unterhalb der letzten Zeile in die neue Textdatei ein. Sobald Sie alle Zertifikate in die neue Textdatei kopiert haben, speichern Sie die Datei im PEM-Format und laden Sie sie auf das Access Gateway hoch.

Erstellen von Stammzertifikaten über eine Eingabeaufforderung

Alternativ können Sie Stammzertifikate im PEM-Format über eine DOS-Eingabeaufforderung erstellen. Wenn Sie drei PEM-Stammzertifikate besitzen, können Sie beispielsweise mit dem nachstehenden Befehl eine einzige Datei mit allen drei Zertifikaten erstellen.

type root1.pem root2.pem root3.pem > current-roots.pem

Sollen weitere Stammzertifikate in eine vorhandene Datei eingefügt werden, verwenden Sie folgenden Befehl:

type root4.pem root5.pem >> current-roots.pem

Nach der Ausführung dieses Befehls befinden sich alle fünf Stammzertifikate in der Datei current-roots.pem. Mit dem zweifachen Größer-als-Zeichen (>>) wird der Inhalt der Dateien root4.pem und root5.pem an den bereits vorhandenen Inhalt der Datei current-roots.pem angehängt.

Konfigurieren weiterer Netzwerkeinstellungen

Nach der Installation der Lizenzen und Zertifikate auf dem Access Gateway fallen ggf. weitere Konfigurationsschritte an, mit denen das Access Gateway auf die Arbeit im Netzwerk vorbereitet wird. Dazu gehören folgende Schritte:

- Konfigurieren von Namensdienstanbietern, mit denen bis zu drei DNS-Server und ein WINS-Server konfiguriert werden können
- Bearbeiten der HOSTS-Datei zum Umgehen des DNS und zum Auflösen bestimmter IP-Adressen in bestimme Hostnamen
- Konfigurieren des dynamischen und statischen Routing für das Abhören von Routen, die von den Routingservern veröffentlicht werden, bzw. für die Verwendung statischer Routen
- Konfigurieren von Datum und Uhrzeit
- Konfigurieren der Standard-Anmeldeseite für den Secure Access Client

Konfigurieren von Namensdienstanbietern

Die Namensauflösung wird auf der Registerkarte **Name Service Providers** konfiguriert. Hier können Sie Einstellungen für bis zu drei DNS-Server und einen WINS-Server angeben.

So legen Sie DNS- und WINS-Server fest:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Name Service Providers**.
3. Geben Sie unter **First DNS server**, **Second DNS Server** oder **Third DNS server** die IP-Adresse der einzelnen Server ein.
4. Geben Sie in das Feld **DNS suffixes** die Suffixe der Server ein.

   Dies sind die DNS-Suffixe der Server. Die einzelnen Einträge in der Liste sind durch ein Leerzeichen voneinander getrennt. Die Syntax für die Einträge lautet: *site.com*. Stellen Sie den Suffixen keinen Punkt (.) voran (Beispiel: .site.com).

   Standardmäßig überprüft das Access Gateway lediglich das Remote-DNS des Benutzers. Wenn ein Failover auf das lokale DNS des Benutzers möglich sein soll, muss Split DNS zugelassen werden. Weitere Informationen finden Sie unter „Aktivieren von Split DNS“ auf Seite 169.
5. Geben Sie in das Feld **WINS Server** die IP-Adresse des Servers ein.
6. Klicken Sie auf **Submit**.

Bearbeiten der HOSTS-Datei

Auf der Registerkarte **Name Service Providers** können Sie Einträge in die HOSTS-Datei des Access Gateways einfügen. Mit den Einträgen in der HOSTS-Datei löst das Access Gateway die vollqualifizierten Domänennamen in IP-Adressen auf.

Beim Umwandeln eines vollqualifizierten Domänennamen in eine IP-Adresse überprüft das Access Gateway zunächst die HOSTS-Datei, bevor eine Verbindung zum DNS-Server aufgebaut wird, um die Adressübersetzung durchzuführen. Wenn der vollqualifizierte Domänenname schon mit den Angaben in der HOSTS-Datei in eine IP-Adresse aufgelöst werden kann, wird der DNS-Server gar nicht erst aufgerufen.

Für den Fall, dass das Access Gateway aufgrund der Netzwerkkonfiguration nicht auf den DNS-Server zugreifen kann, sollten Sie die entsprechenden Einträge in die HOSTS-Datei aufnehmen, damit die Adressauflösung reibungslos abläuft. Dies kann sich außerdem positiv auf die Leistung auswirken, weil das Access Gateway keine Verbindung zu einem anderen Server aufbauen muss, um die Adressen zu übersetzen.

So fügen Sie der HOSTS-Datei einen Eintrag hinzu:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Name Service Providers**.
3. Geben Sie unter **Edit the HOSTS file** in das Feld **IP address** die IP-Adresse ein, die einem bestimmten vollqualifizierten Domänennamen zugewiesen werden soll.
4. Geben Sie in das Feld **FQDN** den vollqualifizierten Domänennamen ein, den Sie mit der im vorigen Schritt eingegebenen IP-Adresse verknüpfen möchten.
5. Klicken Sie auf **Add**.

   Die Gruppe aus IP-Adresse und HOSTS-Name wird in der Hosttabelle aufgeführt.

So entfernen Sie einen Eintrag aus der HOSTS-Datei:

1. Klicken Sie unter **Host Table** auf die Gruppe aus IP-Adresse und HOSTS-Name, die Sie löschen möchten.
2. Klicken Sie auf **Remove**.

Konfigurieren von dynamischen und statischen Routen

Sie können das Access Gateway für das dynamische oder statische Routing konfigurieren. Das Access Gateway unterstützt das dynamische Routing mit dem Routing Information Protocol (RIP und RIP 2).

Aktivieren von dynamischem Routing

Wenn Sie dynamisches Routing für das Access Gateway konfigurieren, passiert Folgendes:

- Das Access Gateway hört Routinginformationen ab, die in Form von RIP-UDP-Paketen veröffentlicht werden. Das Access Gateway füllt die Routingtabelle mit den RIP-Daten.
- Alle vorhandenen statischen Routen werden deaktiviert.

Beim dynamischen Routing können Sie festlegen, dass das dynamische Gateway die Festlegung des vom Access Gateway verwendeten Standardgateways durch RIP zulassen soll. In diesem Fall greift das Access Gateway nicht auf das Standardgateway zurück, das auf der Registerkarte **General Networking** im Administration Tool angegeben ist.

So aktivieren Sie dynamisches Routing:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Wählen Sie unter **Select routing type** die Option **Dynamic routing (RIP)**.
4. Klicken Sie auf **Enable dynamic gateway**, wenn das von den Routingservern bereitgestellte Standardgateway verwendet werden soll.
5. Wählen Sie unter **Routing Interface** den oder die Access Gateway-Netzwerkadapter aus, der oder die für das dynamische Routing verwendet werden soll(en). In der Regel befinden sich die Routingserver innerhalb der Firewall, sodass Sie für diese Einstellung den internen Netzwerkadapter (Interface 1) wählen sollten.
6. Klicken Sie auf **Submit**.

Dynamische Routen werden nicht in der Access Gateway-Routingtabelle aufgeführt.

Aktivieren der RIP-Authentifizierung für das dynamische Routing

Zur Erhöhung der Sicherheit bei dynamischem Routing können Sie das Access Gateway für die RIP-Authentifizierung konfigurieren.

Hinweis: Zur RIP-Authentifizierung muss der RIP-Server RIP-2-Pakete senden; RIP 1 unterstützt die Authentifizierung nicht.

Bei der RIP-Authentifizierung müssen sowohl der RIP-Server als auch das Access Gateway so konfiguriert werden, dass eine bestimmte Authentifizierungs-Zeichenfolge verwendet wird. Der RIP-Server kann diese Zeichenfolge wahlweise als einfachen Text versenden oder auch mit MD5 verschlüsseln.

Falls der RIP-Server die Authentifizierungs-Zeichenfolge mit MD5 verschlüsselt, muss entsprechend die Option für MD5 auf dem Access Gateway aktiviert werden.

Sie können das Access Gateway so konfigurieren, dass es Interface 0 und/oder Interface 1 nach der Zeichenfolge für die RIP-Authentifizierung abhört.

So aktivieren Sie die RIP-Authentifizierung für dynamisches Routing:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Legen Sie die Schnittstelle(n) fest, die das Access Gateway nach der Zeichenfolge für die RIP-Authentifizierung abhören soll. Wählen Sie hierzu unter **Routing Interface** die Option **Interface 0**, **Interface 1** oder **Both**.
4. Aktivieren Sie das Kontrollkästchen **RIP Authentication String for Interface**.
5. Geben Sie in das Textfeld die Authentifizierungs-Zeichenfolge ein, die der RIP-Server übermittelt. Achten Sie dabei auf die exakte Schreibweise und auf die Groß- und Kleinschreibung.
6. Falls der RIP-Server die Authentifizierungs-Zeichenfolge mit MD5 verschlüsselt, aktivieren Sie das Kontrollkästchen **Enable RIP MD5 Authentication for Interface**.

   Aktivieren Sie diese Option nicht, wenn der RIP-Server die Authentifizierungs-Zeichenfolge als reinen Text übermittelt.
7. Klicken Sie auf **Submit**.

Wechseln von dynamischem Routing zu statischem Routing

Bevor Sie von dynamischem Routing zu statischem Routing wechseln, sollten Sie die dynamischen Routen in der statischen Routentabelle speichern. Mit dieser Option werden die aktuellen RIP-Daten zum dynamischen Routing als statische Routen gespeichert.

Wenn Sie von dynamischem Routing zu statischem Routing wechseln und zuvor statische Routen erstellt hatten, werden die statischen Routen in der Routingtabelle des Access Gateways aufgeführt.

Für den Fall, dass diese statischen Routen nicht mehr gültig sind oder noch keine statischen Routen erstellt wurden, geht unter Umständen der Remotezugriff auf das Administration Tool verloren. Die Benutzer können außerdem erst dann wieder auf die Ressourcen im internen Netzwerk zugreifen, wenn Sie die statischen Routen manuell konfiguriert haben.

Durch das Speichern der aktuellen RIP-Daten zum dynamischen Routing wird die Konnektivität beim Wechsel vom dynamischen Routing zum statischen Routing so lange aufrechterhalten, bis Sie die statischen Routen ordnungsgemäß konfiguriert haben.

So speichern Sie dynamische Routen in der Tabelle mit den statischen Routen:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Klicken Sie auf **Save to Static Routes**.

Sobald die dynamischen Routen gespeichert sind, können Sie zum statischen Routing wechseln.

Konfigurieren einer statischen Route

Beim Einrichten der Kommunikation mit einem anderen Host oder Netzwerk muss u. U. eine statische Route vom Access Gateway dem neuen Ziel hinzugefügt werden, sofern Sie kein dynamisches Routing verwenden.

Richten Sie die statischen Routen auf dem Access Gateway-Adapter ein, der nicht von dem auf der Registerkarte **General Networking** angegebenen Standardgateway verwendet wird.

Ein Beispiel für das Einrichten einer statischen Route finden Sie unter „Beispiel für eine statische Route“ auf Seite 68.

So fügen Sie eine statische Route hinzu:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät und klicken Sie auf die Registerkarte **Routes**.
2. Wählen Sie unter **Select routing type** die Option **Static routing**.
3. Geben Sie unter **Add a Static Route** im Feld **Destination LAN IP address** die IP-Adresse des Ziel-LANs ein.
4. Geben Sie unter **Subnet mask** die Subnetzmaske für das Gatewaygerät ein.
5. Geben Sie unter **Gateway** die IP-Adresse für das Standardgateway ein. Wenn Sie kein Gateway angeben, kann das Access Gateway nur auf den Inhalt im lokalen Netzwerk zugreifen.
6. Wählen Sie unter **Interface** den Netzwerkadapter für die statische Route aus. Die Standardeinstellung lautet Interface 0. Klicken Sie auf **Add**.
7. Klicken Sie auf der Registerkarte **General Networking** auf **Submit**.

   Der Routenname wird in der Liste **Static Routes** angezeigt.

So testen Sie eine statische Route:

1. Klicken Sie auf **Start > Ausführen**.
2. Geben Sie im Feld **Öffnen** „cmd“ ein und drücken Sie die **Eingabetaste**.
3. Geben Sie an der Eingabeaufforderung den Befehl **ping *IP-Adresse*** für das Gerät ein, an das der Ping-Befehl gesendet werden soll, und drücken Sie die **Eingabetaste**.

   Wenn eine erfolgreiche Kommunikation mit dem anderen Gerät zustande kommt, wird eine entsprechende Meldung eingeblendet, dass die gleiche Anzahl von Paketen gesendet und empfangen wurde und keine Pakete verloren gegangen sind.

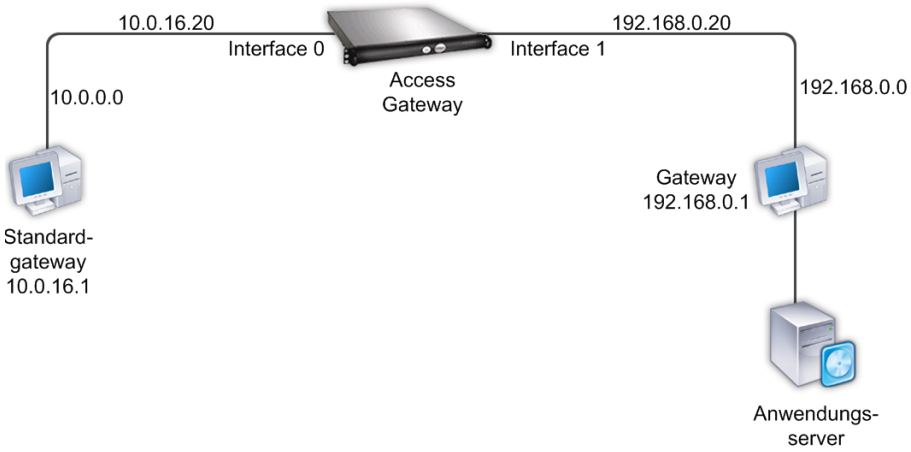
   Wenn keine Kommunikation mit dem anderen Gerät zustande kommt, erhalten Sie Statusmeldungen, aus denen hervorgeht, dass keine Pakete empfangen wurden und dass alle Pakete verloren gegangen sind. Zur Behebung dieses Problems fügen Sie erneut eine statische Route hinzu.

So entfernen Sie eine statische Route:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Wählen Sie in der Tabelle der statischen Routen alle Routen aus, die Sie löschen möchten.
4. Klicken Sie auf **Remove Route**.

Beispiel für eine statische Route

Angenommen, die IP-Adresse für das Interface 0 am Access Gateway lautet 10.0.16.20 und es liegt eine Anforderung für den Zugriff auf Daten auf 129.6.0.20 vor, wofür derzeit kein Pfad vorhanden ist. Vom Netzwerkadapter aus, der nicht als Access Gateway-Standardgateway festgelegt ist, können Sie eine statische Route zur angeforderten Netzwerkadresse erstellen. Die folgende Abbildung enthält eine grafische Darstellung dieser Situation:



Netzwerktopologie mit einer statischen Route

Die Abbildung zeigt die folgenden Verbindungen:

- Der Adapter für Interface 0 (10.0.16.20) führt zum Standardgateway (10.0.16.1), das mit dem übrigen Teil des Netzwerks 10.0.0.0 verbunden ist.
- Der Adapter für Interface 1 (192.168.0.20) ist für die Kommunikation mit dem Netzwerk 192.168.0.0 und dem zugehörigen Gateway (192.168.0.1) eingerichtet. Über dieses Gateway kann das Interface 1 mit dem Netzwerk 129.6.0.20 und dem Server an der IP-Adresse 129.6.0.20 kommunizieren.

Zum Einrichten der statischen Route müssen Sie den Pfad zwischen Interface 1 und der IP-Adresse 129.6.0.20 erstellen.

So richten Sie die statische Beispielroute ein:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Routes**.
3. Wählen Sie ggf. unter **Select routing type** die Option **Static routing**.
4. Legen Sie im Feld **Destination LAN IP address** als IP-Adresse des Ziel-LANs **129.6.0.0** fest.
5. Legen Sie unter **Subnet Mask** die Subnetzmaske für das Gatewaygerät fest.

6. Legen Sie unter **Gateway** als IP-Adresse des Standardgateways **192.168.0.1** fest.
7. Wählen Sie unter **Interface** als Gateway-Geräteadapter die Option **Interface 1** und klicken Sie auf **Add**.
8. Klicken Sie auf der Registerkarte **General Networking** auf **Submit**.

Konfigurieren von Datum und Uhrzeit auf dem Access Gateway

Die Systemuhrzeit wird auf der rechten Seite der Taskleiste im Administration Desktop-Fenster angezeigt. Wenn das Systemdatum angezeigt werden soll, zeigen Sie mit dem Mauszeiger auf die Systemuhrzeit.

Wenn Sie auf die Systemuhrzeit klicken, wird eine Kalenderansicht angezeigt. Diese wird bei erneutem Klicken auf die Systemuhrzeit wieder geschlossen.

So ändern Sie das Systemdatum und die Systemuhrzeit:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Date**.
3. Aktivieren Sie unter **Synchronization Mode** die Option **Manual**.
4. Geben Sie unter **Date** das Datum und die Uhrzeit ein.
5. Wählen Sie unter **Time zone** eine Zeitzone aus.
6. Klicken Sie auf **Submit**.

Konfigurieren eines NTP-Servers

Das Network Time Protocol (NTP) sendet und empfängt Zeitinformationen über TCP/IP-Netzwerke. Es eignet sich daher für die Synchronisierung der internen Uhr von Computern im Netzwerk auf der Basis einer gemeinsamen Referenzzeit.

Wenn sich in Ihrem sicheren Netzwerk ein NTP-Server befindet, können Sie das Access Gateway mit dem Administration Tool so konfigurieren, dass die Uhrzeit des Geräts mit der vom NTP-Server bereitgestellten Zeit synchronisiert wird.

So synchronisieren Sie das Access Gateway mit einem NTP-Server:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Gerät.
2. Klicken Sie auf die Registerkarte **Date**.
3. Aktivieren Sie unter **Synchronization Mode** die Option **Network Time Protocol (NTP)**.
4. Geben Sie in das Feld **NTP server** den vollqualifizierten Domänennamen des Servers ein.
5. Wählen Sie unter **Synchronization interval** einen Zeitplan für die Systemzeitaktualisierungen aus.
6. Klicken Sie auf **Submit**.

Verwenden der Standardportalseite

Die Standardportalseite ist eine HTML-Seite, auf der der Benutzer die Art der Verbindung auswählen kann, die von einem Remotecomputer aus hergestellt werden soll. Die Benutzer können die Verbindung entweder von der Webportalseite aus herstellen oder den Secure Access Client verwenden, der auf ihren Computern installiert ist. Darüber hinaus können sie sich im Kioskmodus anmelden, sofern dieser Modus aktiviert ist.

Weitere Informationen zu den Anmeldeseiten und den verschiedenen Möglichkeiten zum Aufbauen einer Verbindung durch die Clients finden Sie unter „Konfigurieren der Anmelde- und Portalseiten für den Secure Access Client“ auf Seite 183.

Hinweis: Sie können die mit dem Access Gateway bereitgestellten Portalseitenvorlagen individuell anpassen und sie auf Gruppenbasis zuweisen. Informationen hierzu finden Sie unter „Access Gateway-Portalseitenvorlagen“ auf Seite 185. Außerdem können Sie einen Link zu den auf einer Website befindlichen Access Gateway-Clients hinzufügen. Weitere Informationen finden Sie unter „Einfügen von Links zu Clients auf Ihrer Website“ auf Seite 189.

Von der Webportalseite aus startet der Benutzer wahlweise den Secure Access Client oder den Kioskmodus.

- Der Secure Access Client ist für Verbindungen von privaten Computern aus gedacht, weil die Daten aus dem Netzwerk, zu dem der Benutzer eine Verbindung herstellt, an den Computer des Benutzers übertragen werden.
- Der Kioskmodus eignet sich für Verbindungen von einem öffentlichen Computer aus, weil dabei keine Daten auf den Computer des Benutzers geschrieben werden. Wenn Sie jedoch Netzwerkfreigaben konfigurieren, können Benutzer Dateien von einem freigegebenen Netzlaufwerk auf den Remotecomputer kopieren.

Hinweis: Sie können das Access Gateway so konfigurieren, dass die Option, mit der eine Verbindung von einem öffentlichen Computer aus hergestellt wird, für die Benutzer nicht sichtbar ist. Weitere Informationen hierzu finden Sie unter „Verbindungen im Kioskmodus“ auf Seite 157.

So stellen Sie eine Verbindung von der Standardportalseite aus her:

1. Geben Sie in einen Webbrowser die Webadresse für das Access Gateway ein. Beispiel: https://vpn.meinefirma.com.

   Wenn auf dem Access Gateway kein von einer Zertifizierungsstelle signiertes Zertifikat installiert ist, wird das Dialogfeld **Security Alert** angezeigt. Klicken Sie auf **Ja**, um fortzufahren.

2. Geben Sie auf der Anmeldeseite den Benutzernamen und das Kennwort ein und klicken Sie dann auf **Login**.

   Die Standardportalseite wird geöffnet.

   Hinweis: Ist die Option **Enable logon page authentication** auf der Registerkarte **Global Cluster Policies** nicht aktiviert, melden sich die Benutzer erst dann an, wenn die Verbindung zur Portalseite aufgebaut ist (siehe Schritt 3).

   ---

3. So stellen Sie mit dem Secure Access Client eine Verbindung von einem sicheren Computer aus her:

   - Klicken Sie auf **Eigener Computer**.

     Beim ersten Herstellen einer Verbindung über den Webbrowser wird der Client aufgefordert, das ActiveX-Steuerelement net6helper.cab zu installieren. Installieren Sie das ActiveX-Steuerelement.

   - Klicken Sie auf **Speichern** und dann auf **Öffnen**.

     Der Secure Access Client wird auf dem Clientcomputer installiert. Wenn die Verbindung zum Access Gateway zum ersten Mal hergestellt wird, werden die Verwendungsbedingungen für die Software angezeigt. Klicken Sie auf **Annehmen**, um den Treiber zu installieren. Nach der Installation des Treibers kann der Benutzer den Secure Access Client starten, ohne dazu über die Webanmeldung und die Portalseite gehen zu müssen.

   - Klicken Sie auf der Portalseite auf **Verbinden**.

     Die Verbindung ermöglicht es den Benutzern, mit der verbundenen Site genau so zu arbeiten, als wären sie auf der Site selbst angemeldet. Die Daten können zwischen dem Remotecomputer und der verbundenen Site wechselseitig übertragen werden.

4. Falls Sie über einen Webbrowser auf Kioskressourcen zugreifen, klicken Sie auf **Öffentlicher Computer**.

   Die Benutzer geben ihren Benutzernamen und das Kennwort ein und klicken dann auf **Anmelden**. Das Kiosk-Fenster wird geöffnet. Standardmäßig ist diese Option nicht verfügbar. Weitere Informationen zum Aktivieren des Kioskmodus finden Sie unter „Verbindungen im Kioskmodus“ auf Seite 157.

Wenn Sie den Secure Access Client für die automatische Anmeldung an Windows konfiguriert haben, wird der Client gestartet, sobald die Benutzer ihre Windows-Anmeldeinformationen eingegeben haben. Diese Anmeldeinformationen werden auch für den Secure Access Client verwendet. Das bedeutet, dass die Benutzer beim Starten des Computers die Authentifizierung nicht wiederholen müssen, um eine Verbindung herzustellen, vorausgesetzt, die Benutzer verfügen über eine Netzwerkverbindung und sie können sich an Windows anmelden. Weitere Informationen zur Konfiguration der Single Sign-On-Funktion unter Windows finden Sie unter „Konfigurieren von Single Sign-on für Windows-Betriebssysteme“ auf Seite 149.

Installieren des Secure Access Client für Linux

Wenn Sie eine Verbindung von einem Linux-Computer aus herstellen, klicken Sie auf den Linux-Downloadlink. Damit wird der Downloadvorgang gestartet und Sie erhalten Anweisungen zum Installieren des Clients.

Hinweis: Der Secure Access Client benötigt die Linux-Pakete tcl und tk.

Neben dem Befehl net6vpn --login, mit dem das Anmeldedialogfeld für den Secure Access Client geöffnet wird, können Sie auch den Befehl **net6vpn** eingeben. Hiermit rufen Sie eine Liste weiterer Befehlszeilenoptionen auf. Wenn die Verbindung getrennt wird, wird der VPN-Dämon u. U. gestoppt. Der Secure Access Client benötigt zum Herstellen einer Verbindung zum Access Gateway jedoch einen laufenden VPN-Dämon. Wenn Sie den Status des VPN-Dämons prüfen möchten, geben Sie an einer Eingabeaufforderung Folgendes ein:

/sbin/service net6vpnd status

Zum Neustarten eines gestoppten Dämons geben Sie Folgendes ein:

/sbin/service net6vpnd start

So entfernen Sie den Linux-VPN-Client:

1. Geben Sie an einer Eingabeaufforderung Folgendes ein:

   /sbin/service net6vpnd stop
   /sbin/chkconfig -del net6vpnd
   rm -rf /etc/net6vpn.conf /etc/init.d/net6vpnd /usr/bin/net6vpn /usr/sbin/net6vpnd /usr/local/net6vpn/

Konfigurieren des Netzwerkzugriffs

Nachdem das Gerät für den Betrieb in der Netzwerkumgebung konfiguriert wurde, konfigurieren Sie den Netzwerkzugriff für das Gerät sowie für die Gruppen und Benutzer.

So konfigurieren Sie den Netzwerkzugriff:

Schritt 1: Konfigurieren der Netzwerke, zu denen die Clients eine Verbindung aufbauen können: Standardmäßig können die Clients keine Verbindungen zu einem Netzwerk herstellen. Als ersten Schritt beim Konfigurieren des Netzwerkzugriffs legen Sie auf der Registerkarte **Global Cluster Policies** die Netzwerke fest, zu denen die Clients eine Verbindung herstellen sollen.

Schritt 2: Konfigurieren der Authentifizierung und Autorisierung: Mit der Authentifizierung wird definiert, wie die Benutzer sich anmelden; die Konfiguration erfolgt mit Bereichen. Die folgenden Authentifizierungsarten stehen zur Auswahl: lokal, NTLM, LDAP, RADIUS, RSA SecurID und SafeWord. Bei der Autorisierung stehen die folgenden Optionen zur Verfügung: lokal, LDAP, RADIUS, NTLM, keine Autorisierung. Weitere Informationen zur Konfiguration der Authentifizierung und Autorisierung finden Sie unter „Konfigurieren der Authentifizierung und Autorisierung“ auf Seite 77.

Schritt 3: Konfigurieren von Benutzergruppen: Benutzergruppen kommen im Zusammenhang mit der Autorisierung zum Einsatz. Wenn die Benutzer ihre Verbindungen beispielsweise über LDAP herstellen, legen Sie einen LDAP-Autorisierungsbereich an und erstellen Sie dann eine Gruppe. Die Namen der Benutzergruppen müssen mit den Namen dieser Gruppen auf dem LDAP-Server übereinstimmen. Darüber hinaus können Sie lokale Benutzer zur lokalen Authentifizierung auf dem Access Gateway anlegen. Die lokalen Benutzer werden dann Benutzergruppen hinzugefügt. Weitere Informationen zum Konfigurieren lokaler Benutzer finden Sie unter „Konfigurieren lokaler Benutzer“ auf Seite 84.

Schritt 4: Konfigurieren des Netzwerkzugriffs für Gruppen: Konfigurieren Sie den Netzwerkzugriff für die erstellten Benutzergruppen. Hierzu gehören die Netzwerkressourcen, auf die die Benutzer in der Gruppe zugreifen können, außerdem die Anwendungsrichtlinien, die Kioskverbindungen und die Endpunktrichtlinien.

Weitere Informationen zum Konfigurieren von zugänglichen Netzwerken, Benutzergruppen und Netzwerkzugriff für Benutzer finden Sie unter „Konfigurieren von Netzwerkzugriff und Gruppenressourcen“ auf Seite 113.

Citrix empfiehlt, sich mit den Szenarien unter „Beispiele für die Konfiguration des Netzwerkzugriffs“ auf Seite 307 vertraut zu machen, bevor Sie den Netzwerkzugriff für das Gerät konfigurieren.

KAPITEL 6

Konfigurieren der Authentifizierung und Autorisierung

Das Access Gateway unterstützt verschiedene Authentifizierungstypen: LDAP, RADIUS, RSA SecurID, NTLM und die SafeWord-Produkte von Secure Computing.

In den folgenden Themen wird die Vorgehensweise bei der Konfigurierung der Authentifizierung in Access Gateway beschrieben:

- Voraussetzungen zum Konfigurieren der Authentifizierung auf dem Access Gateway
- Konfigurieren der Authentifizierung auf dem Access Gateway
- Konfigurieren der lokalen Authentifizierung
- Konfigurieren lokaler Benutzer
- Konfigurieren von LDAP-Authentifizierung und -Autorisierung
- Konfigurieren von RADIUS-Authentifizierung und -Autorisierung
- Konfigurieren der RSA SecurID-Authentifizierung
- Konfigurieren der Authentifizierung mit Secure Computing SafeWord
- Konfigurieren von NTLM-Authentifizierung und -Autorisierung
- Konfigurieren von Zweimethodenauthentifizierung

Voraussetzungen zum Konfigurieren der Authentifizierung auf dem Access Gateway

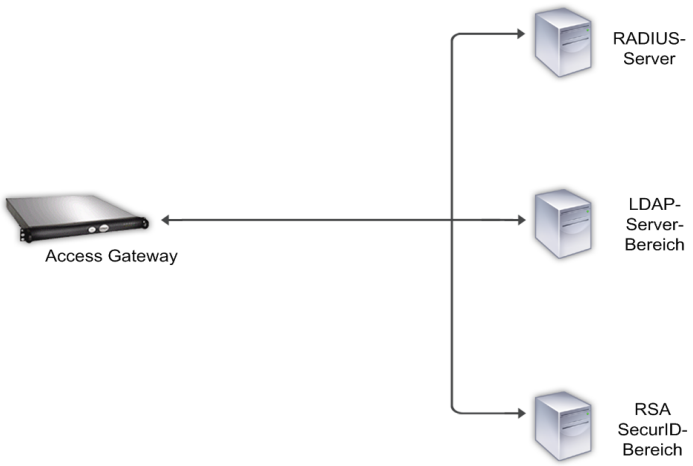
Wenn für die Gruppe des Benutzers keine dieser Authentifizierungsmethoden konfiguriert ist, erfolgt die Authentifizierung anhand der lokalen Benutzerauthentifizierungsdatenbank des Access Gateways. Die Authentifizierung wird in den folgenden Fällen auf dem Access Gateway konfiguriert:

- Das Access Gateway wird in der DMZ oder im sicheren Netzwerk bereitgestellt und die Benutzer stellen eine direkte Verbindung zum Gerät her.
- Das Access Gateway wird in der DMZ bereitgestellt und das Webinterface befindet sich ebenfalls in der DMZ hinter dem Access Gateway.
- Das Access Gateway wird in der DMZ und das Webinterface im sicheren Netzwerk bereitgestellt.

Wenn das Webinterface parallel zum Access Gateway verwendet wird oder das Gerät zur Verwendung von Citrix Presentation Server Clients konfiguriert ist und das Webinterface Verbindungen zu veröffentlichten Anwendungen in einer Serverfarm herstellt, besteht die Möglichkeit, die Autorisierung auf dem Access Gateway zu konfigurieren.

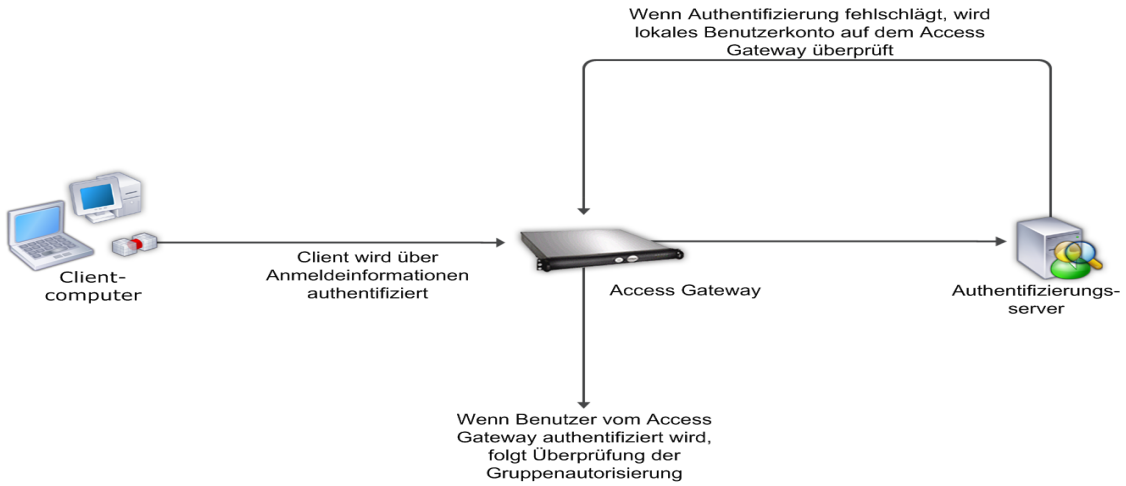
Konfigurieren der Authentifizierung auf dem Access Gateway

Standardmäßig authentifiziert das Access Gateway die Benutzer anhand einer lokal im Access Gateway gespeicherten Benutzerliste. Sie können das Access Gateway für die Verwendung von LDAP-, RADIUS-, RSA SecurID-, SafeWord- oder NTLM (Windows NT 4.0)-Authentifizierungsservern konfigurieren. Das Access Gateway unterstützt die bereichsbasierte Authentifizierung, sodass auch Sites mit mehr als einem LDAP- oder RADIUS-Server oder mit einer Kombination aus SafeWord-, LDAP-, RADIUS-, NTLM- und/oder RSA SecurID-Authentifizierungsservern unterstützt werden.



Kommunikation zwischen Access Gateway und Authentifizierungsservern

Wenn sich ein Benutzer nicht auf dem Authentifizierungsserver befindet oder wenn die Authentifizierung auf diesem Server fehlschlägt, versucht das Access Gateway, den Benutzer anhand der lokalen Benutzerliste zu authentifizieren, wenn auf der Registerkarte **Authentication > Settings** das Kontrollkästchen **Use the local user database on the Access Gateway** aktiviert ist.



Kommunikation zwischen dem Client, dem Access Gateway und dem lokalen Benutzerkonto bei Fehlschlagen der Authentifizierung auf dem Authentifizierungsserver

Nach der Authentifizierung eines Benutzers führt das Access Gateway eine Gruppenautorisierung durch. Dazu werden die Informationen der Gruppe des Benutzers von einem LDAP-Server, einem RADIUS-Server, einem Windows NT 4.0-Server (zur NTLM-Autorisierung) oder der lokalen Gruppendatei (sofern nicht auf dem LDAP- oder RADIUS-Server verfügbar) abgerufen. Wenn für den Benutzer Gruppeninformationen verfügbar sind, überprüft das Access Gateway anschließend die für die Gruppe zulässigen Netzwerkressourcen. Die LDAP-Autorisierung kann mit allen unterstützten Authentifizierungsmethoden verwendet werden.

Die vom LDAP-Server abgerufenen Gruppennamen werden mit den Gruppennamen verglichen, die lokal im Access Gateway erstellt wurden. Wenn die Gruppennamen übereinstimmen, werden die Eigenschaften der lokalen Gruppe auf die Gruppe angewendet, die von den LDAP-Servern abgerufen wurde.

Konfigurieren der Authentifizierung ohne Autorisierung

Das Access Gateway kann so konfiguriert werden, dass Benutzer authentifiziert werden, ohne dass eine Autorisierung erforderlich ist. Wenn ein Benutzer nicht autorisiert ist, führt das Access Gateway keine Gruppenautorisierung durch. Dem Benutzer werden die Einstellungen der Standardbenutzergruppe zugewiesen.

So stellen Sie auf dem Access Gateway ein, dass keine Autorisierung erforderlich ist:

1. Wählen Sie auf der Registerkarte **Authentication** einen Autorisierungsbereich aus.
2. Klicken Sie auf die Registerkarte **Authorization** und wählen Sie unter **Authorization type** die Option **No authorization**.

Konfigurieren des Bereichs „Default“

Das Access Gateway verfügt über einen permanenten Bereich mit der Bezeichnung **Default**. Der Bereich **Default** ist für lokale Authentifizierung vorkonfiguriert. Wenn Sie die Authentifizierungsmethode des Bereichs **Default** ändern möchten, muss dieser sofort durch einen neuen Bereich **Default** ersetzt werden.

Der Bereich **Default** wird verwendet, wenn ein Benutzer bei der Anmeldung am Access Gateway lediglich einen Benutzernamen eingibt. Bei allen anderen Bereichen muss beim Anmelden ein Bereichsname eingegeben werden. Wenn sich die meisten Benutzer bei einem nicht-lokalen Authentifizierungsbereich anmelden, sollten Sie daher den Authentifizierungstyp für den Bereich **Default** ändern.

Entfernen Sie zum Ändern des Authentifizierungstyps des Bereichs **Default** diesen Bereich und erstellen Sie dann sofort einen neuen mit der entsprechenden Authentifizierungskonfiguration.

So können Sie den Bereich „Default“ entfernen und neu erstellen:

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Öffnen Sie das Fenster für den Bereich **Default**.
3. Wählen Sie im Menü **Action** den Befehl **Remove Default realm**.

   Es wird eine Warnmeldung angezeigt. Klicken Sie auf **Ja**.
4. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** „Default“ ein.

Hinweis: Beim Erstellen eines neuen Bereich **Default** muss beim Wort „Default“ die Groß- und Kleinschreibung beachtet und ein großes „D“ verwendet werden.

---

5. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie einen einzelnen Authentifizierungstyp konfigurieren, wählen Sie **One Source** aus und klicken Sie auf **Add**.
   - Wenn Sie Zweimethodenauthentifizierung konfigurieren, wählen Sie **Two Source** aus und klicken Sie auf **Add**.
6. Wählen Sie unter **Authentication type** den Authentifizierungstyp aus und klicken Sie dann auf **OK**.
7. Konfigurieren Sie die Authentifizierungseinstellungen. Weitere Informationen finden Sie in den folgenden Abschnitten:
   - „Konfigurieren der lokalen Authentifizierung“ auf Seite 83
   - „Konfigurieren von LDAP-Authentifizierung und -Autorisierung“ auf Seite 86
   - „Konfigurieren von RADIUS-Authentifizierung und -Autorisierung“ auf Seite 95
   - „Konfigurieren der RSA SecurID-Authentifizierung“ auf Seite 100
   - „Konfigurieren der Authentifizierung mit Secure Computing SafeWord“ auf Seite 104
   - „Konfigurieren von NTLM-Authentifizierung und -Autorisierung“ auf Seite 107

Erstellen von zusätzlichen Bereichen

Neben dem Bereich **Default** können noch weitere Bereiche erstellt werden. Beispiel: Der Bereich **Default** soll für die Authentifizierung bei einem LDAP-Server verwendet werden. Wenn Sie für die Benutzer zusätzliche Authentifizierungsmethoden verwenden möchten, wie z. B. RADIUS, SafeWord, RSA SecurID, NTLM oder lokale Authentifizierung am Gerät, können Sie für jede dieser Methoden einen Bereich erstellen. Wenn sich ein Benutzer an anderen Bereichen als dem Bereich **Default** anmeldet, muss er den Namen des Bereichs und seinen Benutzernamen eingeben, z. B. *Bereichsname\Benutzername*.

Hinweis: Citrix empfiehlt, die Bereiche nach den dazugehörigen Domänen zu benennen. Dadurch können sich Benutzer entweder mit *Bereichsname\Benutzername* oder mit *Benutzername@Bereichsname* anmelden.

So erstellen Sie einen Bereich:

1. Geben Sie auf der Registerkarte **Authentication** unter **Add an Authentication Realm** in das Feld **Realm name** den Namen des Bereichs ein.
2. Führen Sie einen der folgenden Schritte aus:

   Wenn die Benutzer nur einen Authentifizierungstyp verwenden, klicken Sie auf **One Source**.

   - oder -

   Wenn die Benutzer zwei Authentifizierungstypen verwenden, klicken Sie auf **Two Source**.
3. Klicken Sie auf **Add**.
4. Wählen Sie unter **Authentication type** die Authentifizierungsmethode aus und klicken Sie auf **OK**.

   Wenn Sie Zweimethodenauthentifizierung konfigurieren, wählen Sie unter **Primary authentication type** den Typ aus, mit dem sich Benutzer zuerst anmelden. Wählen Sie unter **Secondary authentication type** den Typ aus, mit dem sich die Benutzer als zweites anmelden. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Zweimethodenauthentifizierung“ auf Seite 110.
5. Konfigurieren Sie die Einstellungen für den Bereich und klicken Sie dann auf **Submit**.

Entfernen von Bereichen

Wenn Sie einen Authentifizierungsserver außer Betrieb nehmen oder einen Domänenserver entfernen, können Sie jeden Bereich mit Ausnahme des Bereichs **Default** entfernen. Den Bereich **Default** können Sie nur entfernen, wenn Sie sofort wieder einen neuen Bereich mit diesem Namen erstellen. Weitere Informationen hierzu finden Sie unter „Konfigurieren des Bereichs „Default““ auf Seite 80.

So entfernen Sie einen Bereich:

1. Öffnen Sie auf der Registerkarte **Authentication** den Bereich, der entfernt werden soll.
2. Klicken Sie im Menü **Action** auf **Remove *Bereichsname* realm**.

   Der Bereich wird entfernt.

Konfigurieren der lokalen Authentifizierung

Bei einer Neuinstallation wird für den Bereich **Default** die lokale Authentifizierung festgelegt. Auf diese Weise können sich die Benutzer am Access Gateway anmelden, ohne einen Bereichsnamen eingeben zu müssen.

Wenn einige Benutzer sich ausschließlich anhand der lokalen Benutzerliste des Access Gateways authentifizieren, können Sie für den Bereich **Default** die lokale Authentifizierung beibehalten. Sie können alternativ dazu auch einen anderen Bereich für die lokale Authentifizierung erstellen und den Bereich **Default** dann für einen anderen Authentifizierungstyp verwenden. Informationen hierzu finden Sie unter „So können Sie den Bereich „Default“ entfernen und neu erstellen:“ auf Seite 81.

Wenn sich alle Benutzer unter Verwendung von Authentifizierungsservern authentifizieren, wird kein Bereich für die lokale Authentifizierung benötigt. Das Access Gateway kann die lokale Benutzerdatenbank auf dem Gerät nach Authentifizierungsinformationen überprüfen, wenn die Authentifizierung eines Benutzers auf einem anderen Authentifizierungsserver fehlschlägt. Wenn Sie z. B. LDAP verwenden und die Authentifizierung fehlschlägt, können sich die Benutzer mit der lokalen Benutzerdatenbank anmelden.

So stellen Sie die Authentifizierung mit der lokalen Benutzerliste auf dem Access Gateway ein:

1. Öffnen Sie auf der Registerkarte **Authentication** den Authentifizierungsbereich, in dem Sie lokale Authentifizierung konfigurieren möchten.
2. Klicken Sie auf die Registerkarte **Settings**.
3. Aktivieren Sie die Option **Use the local user database on the Access Gateway**.
4. Klicken Sie auf **Submit**.

Hinweis: Dieses Kontrollkästchen steht nicht zur Verfügung, wenn der Bereich für lokale Authentifizierung konfiguriert ist.

Konfigurieren lokaler Benutzer

Sie können auf dem Access Gateway lokale Benutzerkonten erstellen und so die Liste der Benutzer auf den Authentifizierungsservern ergänzen. So können Sie beispielsweise lokale Benutzerkonten für temporäre Benutzer, wie z. B. Unternehmensberater oder Besucher, erstellen, ohne auf dem Authentifizierungsserver einen Eintrag für diese Benutzer erstellen zu müssen. In diesem Fall fügen Sie den Benutzer der lokalen Benutzerliste des Access Gateways hinzu. Dies wird weiter unten ausführlicher beschrieben.

Wenn Sie einen Benutzer einer anderen Gruppe hinzufügen möchten, klicken Sie unter **Local Users** auf den Benutzer und ziehen Sie ihn auf die entsprechende Benutzergruppe.

Wenn der Benutzer keiner der von Ihnen auf dem Access Gateway definierten Gruppen angehört, werden ihm die Einstellungen der Standardbenutzergruppe zugewiesen. Wenn der Benutzer einer anderen Gruppe als der Standardgruppe angehört, werden ihm nur dann die Einstellungen der Standardgruppe zugewiesen, wenn seine Gruppe zur Übernahme dieser Einstellungen konfiguriert wurde. Weitere Informationen hierzu finden Sie unter „Eigenschaften der Standardgruppe („Default“)“ auf Seite 122.

So erstellen Sie einen Benutzer auf dem Access Gateway:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **Local Users** und klicken Sie dann auf **New User**.

3. Geben Sie unter **User Name** einen Benutzernamen ein. Benutzernamen können Leerzeichen enthalten.

Hinweis: Bei Benutzernamen muss die Groß- und Kleinschreibung nicht beachtet werden. Die Verwendung von Schrägstrichen (/) ist in Benutzernamen und Kennwörtern nicht zulässig. Kennwörter dürfen nicht mit einem Leerzeichen beginnen oder enden.

---

4. Geben Sie in die Felder **Password** und **Verify Password** das Kennwort für den Benutzer ein.

   Dieses Kennwort muss der Benutzer bei der Anmeldung eingeben. Kennwörter müssen zwischen 6 und 127 Zeichen lang sein.

5. Klicken Sie auf **OK**.

So löschen Sie einen Benutzer vom Access Gateway:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie im linken Bereich in der Liste **Local Users** mit der rechten Maustaste auf den entsprechenden Benutzer und klicken Sie dann auf **Remove**.

Zuweisen von Benutzern zu mehreren Gruppen

Nachdem Sie die lokale Benutzerliste erstellt haben, können Sie die Benutzer den auf dem Access Gateway erstellten Gruppen hinzufügen.

Wenn Sie mehrere Gruppen mit einem Benutzerkonto verknüpfen, werden für den Benutzer die Eigenschaften der ersten auf der Registerkarte **Group Priority** ausgewählten Gruppe verwendet.

So fügen Sie einen Benutzer einer Gruppe hinzu:

Klicken Sie in der Liste **Local Users** auf den Benutzer und ziehen Sie ihn auf eine Gruppe.

Ändern von Kennwörtern für Benutzer

Im Administration Tool können Sie das Kennwort eines Benutzers ändern.

So ändern Sie das Kennwort eines Benutzers:

1. Klicken Sie auf der Registerkarte **Access Policy Manager** mit der rechten Maustaste auf einen Benutzer und klicken Sie dann auf **Set Password**.
2. Geben Sie das Kennwort zweimal ein und klicken Sie dann auf **OK**.

Konfigurieren von LDAP-Authentifizierung und -Autorisierung

Sie können das Access Gateway für die Authentifizierung des Benutzerzugriffs mit einem oder mehreren LDAP-Servern konfigurieren. Wenn ein Benutzer sich nicht in einem LDAP-Verzeichnis befindet oder wenn die Authentifizierung bei einem Server fehlschlägt, überprüft das Access Gateway die Anmeldeinformationen des Benutzers anhand der lokal im Access Gateway gespeicherten Benutzerinformationen.

Für die LDAP-Autorisierung müssen die Gruppennamen in Active Directory, auf dem LDAP-Server und auf dem Access Gateway übereinstimmen (inklusive Leerzeichen und Groß-/Kleinschreibung).

Die LDAP-Authentifizierung wird standardmäßig mit SSL/TLS gesichert. Es gibt zwei Arten sicherer LDAP-Verbindungen. Bei der einen Art nimmt der LDAP-Server die SSL/TLS-Verbindung auf einem anderen als dem Port an, der zur Annahme unverschlüsselter LDAP-Verbindungen verwendet wird. Wenn ein Client die SSL/TLS-Verbindung herstellt, kann der LDAP-Verkehr über diese Verbindung gesendet werden. Bei der zweiten Art sind sowohl unsichere als auch sichere LDAP-Verbindungen zulässig, wobei die Verbindungen alle über denselben Serverport laufen. In diesem Fall muss der Client zum Herstellen einer sicheren Verbindung zunächst eine unverschlüsselte LDAP-Verbindung einrichten. Anschließend wird über diese Verbindung der LDAP-Befehl *StartTLS* an den Server gesendet. Wenn der LDAP-Server *StartTLS* unterstützt, wird die Verbindung in eine sichere LDAP-Verbindung mit TLS umgewandelt.

Für LDAP-Verbindungen werden die folgenden Portnummern verwendet:

- 389 für unsichere LDAP-Verbindungen
- 636 für sichere LDAP-Verbindungen
- 3268 für unsichere LDAP-Verbindungen unter Microsoft
- 3269 für sichere LDAP-Verbindungen unter Microsoft

LDAP-Verbindungen, die den Befehl StartTLS verwenden, nutzen die Portnummer 389. Wenn die Portnummern 389 oder 3268 auf dem Access Gateway konfiguriert sind, wird versucht, die Verbindung mit StartTLS herzustellen. Bei Verwendung einer anderen Portnummer erfolgen die Verbindungsversuche mittels SSL/TLS. Können StartTLS oder SSL/TLS nicht verwendet werden, kann die Verbindung nicht hergestellt werden.

Hinweis: Wenn das Access Gateway von Version 4.0 oder 4.1 aktualisiert wird und bereits ein LDAP-Bereich konfiguriert ist, sind die LDAP-Verbindungen standardmäßig nicht gesichert. Wenn das Access Gateway jedoch neu installiert wurde oder wenn Sie einen neuen LDAP-Bereich erstellen, sind die LDAP-Verbindungen standardmäßig sicher.

Beim Konfigurieren des LDAP-Servers muss die Groß- und Kleinschreibung mit der Schreibung auf dem Server und auf dem Access Gateway identisch sein. Wenn das Stammverzeichnis des LDAP-Servers festgelegt wird, wird auch in allen Unterverzeichnissen nach dem Benutzerattribut gesucht. In großen Verzeichnissen kann sich dies negativ auf die Arbeitsgeschwindigkeit auswirken. Citrix empfiehlt daher die Verwendung einer spezifischen Organisationseinheit.

Die folgende Tabelle enthält Beispiele für Benutzerattributfelder für LDAP-Server:

LDAP-Server	**Benutzerattribut**	**Groß-/Kleinschreibung relevant**
Microsoft Active Directory-Server	sAMAccountName	Nein
Novell eDirectory	cn	Ja
IBM Directory Server	uid	
Lotus Domino	CN	
Sun ONE-Verzeichnis (früher iPlanet)	uid oder cn	Ja

Die folgende Tabelle enthält Beispiele für den Basis-DN:

LDAP-Server	**Basis-DN**
Microsoft Active Directory-Server	DC=citrix, DC=local
Novell eDirectory	dc=citrix,dc=net
IBM Directory Server	
Lotus Domino	OU=City, O=Citrix, C=US
Sun ONE-Verzeichnis (früher iPlanet)	ou=People,dc=citrix,dc=com

Die folgende Tabelle enthält Beispiele für den Bind-DN:

LDAP-Server	Bind-DN
Microsoft Active Directory-Server	CN=Administrator, CN=Users, DC=citrix, DC=local
Novell eDirectory	cn=admin, dc=citrix, dc=net
IBM Directory Server	
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE-Verzeichnis (früher iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

Hinweis: Weitere Informationen zu LDAP-Servereinstellungen finden Sie unter „Bestimmen der Attribute in Ihrem LDAP-Verzeichnis“ auf Seite 94.

So erstellen Sie einen LDAP-Authentifizierungsbereich:

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen für den Authentifizierungsbereich ein.

   Wenn Ihre Site mehrere Authentifizierungsbereiche besitzt, sollten Sie einen Namen verwenden, aus dem deutlich der LDAP-Bereich hervorgeht, für den Sie die Einstellungen festlegen. Bei Bereichsnamen ist auf die Groß- und Kleinschreibung zu achten. Darüber hinaus können sie Leerzeichen enthalten.

   Hinweis: Wenn der Bereich **Default** die LDAP-Authentifizierung verwenden soll, entfernen Sie den Bereich **Default** wie unter „So können Sie den Bereich „Default“ entfernen und neu erstellen:“ auf Seite 81 beschrieben.

3. Wählen Sie **One Source** und klicken Sie auf **Add**.
4. Wählen Sie im Dialogfeld **Select Authentication Type** unter **Authentication Type** die Option **LDAP authentication** und klicken Sie auf **OK**.

   Ein Dialogfeld mit dem Namen des neuen Bereichs wird geöffnet.

Konfigurieren Sie nach der Erstellung des Bereichs die LDAP-Authentifizierung.

So konfigurieren Sie die LDAP-Authentifizierung:

1. Geben Sie unter **IP address** die IP-Adresse des LDAP-Servers ein.
2. Geben Sie im Feld **Port** die Portnummer ein.

   Der Standardport für den LDAP-Server ist 389. Wenn Sie eine indexierte Datenbank verwenden, wie z. B. Microsoft Active Directory mit einem globalen Katalog, können Sie durch Ändern des LDAP-Serverports zu 3268 die Geschwindigkeit der LDAP-Abfragen deutlich erhöhen.

   Wenn Ihr Verzeichnis nicht indexiert ist, empfiehlt Citrix anstelle einer anonymen Verbindung zwischen dem Access Gateway und der Datenbank die Verwendung einer administrativen Verbindung. Die Verwendung einer solchen Verbindung verbessert die Downloadgeschwindigkeit.
3. Führen Sie einen der folgenden Schritte aus:

   - Um unsichere LDAP-Verbindungen zuzulassen, aktivieren Sie die Option **Allow Unsecure Connection**.
   - Um LDAP-Verbindungen zu sichern, deaktivieren Sie die Option **Allow Unsecure Connection**.

     Wenn diese Option nicht aktiviert ist, sind alle LDAP-Verbindungen sicher.
4. Geben Sie unter **Administrator Bind DN** den Administrator-Bind-DN für Abfragen ein, die an Ihr LDAP-Verzeichnis gerichtet sind.

   Die Syntax für den Bind-DN kann z. B. wie folgt aussehen:
   Domäne/Benutzername
   ou=Administrator,dc=ace,dc=com
   Benutzer@Domäne.Name (für Active Directory)
   cn=Administrator,cn=Users,dc=ace,dc=com

   Für Active Directory muss der Gruppenname wie folgt angegeben werden: cn=*Gruppenname*. Der auf dem Access Gateway definierte Gruppenname muss identisch mit dem auf dem LDAP-Server definierten Gruppennamen sein.

   Bei anderen LDAP-Verzeichnissen ist der Gruppenname entweder nicht erforderlich oder er muss, sofern er doch nötig ist, in folgender Form angegeben werden: „ou=*Gruppenname*“.

   Das Access Gateway registriert sich mit den Administratoranmeldeinformationen beim LDAP-Server und sucht dann nach dem Benutzer. Wenn der Benutzer gefunden ist, hebt das Access Gateway die Registrierung mit den Administratoranmeldeinformationen auf und registriert sich erneut mit den Benutzeranmeldeinformationen.
5. Geben Sie unter **Administrator password** das Kennwort ein.

6. Geben Sie unter **Base DN (location of users)** den Basis-DN für die Benutzer ein.

   Der Basis-DN wird normalerweise vom Bind-DN abgeleitet, indem der Benutzername entfernt und die Gruppe angegeben wird, in der sich die Benutzer befinden. Die Syntax für den Basis-DN kann z. B. wie folgt aussehen:
   ou=users,dc=ace,dc=com
   cn=Users,dc=ace,dc=com

7. Geben Sie unter **Server logon name attribute** das Attribut ein, unter dem das Access Gateway nach den Benutzeranmeldenamen für den LDAP-Server suchen soll, den Sie gerade konfigurieren. Das Standardattribut ist **sAMAccountName**. Wenn Sie andere Verzeichnisse verwenden, verwenden Sie als Attribut **cn**. Klicken Sie auf **Submit**.

Das Access Gateway kann so konfiguriert werden, dass der Benutzerzugriff mit einem oder mehreren LDAP-Server(n) authentifiziert wird. Wenn sich ein Benutzer nicht in einem LDAP-Verzeichnis befindet oder wenn die Authentifizierung auf einem Server fehlschlägt, überprüft das Access Gateway den Benutzer anhand der lokal auf dem Access Gateway gespeicherten Benutzerinformationen, sofern auf der Registerkarte **Settings** die Option **Use the local user database on the Access Gateway** aktiviert ist.

Für die LDAP-Autorisierung müssen die Gruppennamen in Active Directory, auf dem Access Gateway und auf dem LDAP-Server identisch sein (inklusive Leerzeichen und Groß-/Kleinschreibung).

Hinweis: Weitere Informationen zur Festlegung der LDAP-Servereinstellungen finden Sie unter „Bestimmen der Attribute in Ihrem LDAP-Verzeichnis“ auf Seite 94.

Konfigurieren der LDAP-Autorisierung

Im Folgenden werden die LDAP-Gruppenmitgliedschaftsattribute beschrieben, die mit der Access Gateway-Autorisierung funktionieren und nicht funktionieren.

Für die LDAP-Authentifizierung können Sie die folgenden Autorisierungstypen verwenden:

- Lokale Autorisierung
- LDAP-Autorisierung
- Keine Autorisierung

Wenn Sie die Zweimethodenauthentifizierung verwenden, basiert die Autorisierung auf der primären, nicht der sekundären Authentifizierungsmethode.

Auswertung der Gruppenmitgliedschaft anhand von Gruppenobjekten

Einige LDAP-Server, die die Gruppenmitgliedschaft indirekt anhand von Gruppenobjekten auswerten, können die Access Gateway-Autorisierung verwenden.

Es gibt LDAP-Server, bei denen die Benutzerobjekte Informationen zu den Gruppen enthalten können, zu denen sie gehören. Dazu gehören z. B. Active Directory und eDirectory. Die Gruppenmitgliedschaft eines Benutzers kann aus berechenbaren Attributen aus dem Benutzerobjekt hervorgehen, wie das z. B. beim IBM Directory Server oder beim Sun ONE-Verzeichnisserver der Fall ist. Bei einigen LDAP-Servern kann dieses Attribut verwendet werden, um die dynamische Gruppenmitgliedschaft, die verschachtelte Gruppenmitgliedschaft und die statische Gruppenmitgliedschaft eines Benutzers einzuschließen, sodass alle Gruppenmitgliedschaften anhand eines einzelnen Attributs gefunden werden können.

So können z. B. in IBM Directory Server alle Gruppenmitgliedschaften (in statischen, dynamischen und verschachtelten Gruppen) über das Attribut **ibm-allGroups** zurückgegeben werden. In Sun ONE werden alle Rollen, einschließlich der verwalteten, gefilterten und verschachtelten Rollen, mit dem Attribut *nsRole* berechnet.

Auswertung der Gruppenmitgliedschaft anhand von Gruppenobjekten ohne Access Gateway-Autorisierung

Einige LDAP-Server, die die Gruppenmitgliedschaft indirekt anhand von Gruppenobjekten auswerten, verwenden die Access Gateway-Autorisierung nicht.

Es gibt LDAP-Server, bei denen nur Gruppenobjekte Informationen über Benutzer enthalten können (z. B. der Lotus Domino-LDAP-Server). Das Benutzerobjekt darf bei diesen LDAP-Servern keine Informationen über Gruppen enthalten. Bei solchen LDAP-Servern erfolgt die Suche nach der Gruppenmitgliedschaft, indem der Benutzer in der Mitgliederliste der Gruppen gesucht wird.

Gruppenattributfelder für die LDAP-Autorisierung

Die folgende Tabelle enthält Beispiele für LDAP-Gruppenattributfelder.

Microsoft Active Directory-Server	memberOf
Novell eDirectory	groupMembership
IBM Directory Server	ibm-allGroups
Sun ONE-Verzeichnis (früher iPlanet)	nsRole

So konfigurieren Sie die LDAP-Autorisierung:

1. Klicken Sie auf die Registerkarte **Authorization**.
2. Wählen Sie unter **Authorization type** die Option **LDAP authorization**.
3. Geben Sie unter **IP address** die IP-Adresse des LDAP-Servers ein.
4. Geben Sie im Feld **Port** die Portnummer ein. Der Standardport ist 389.
5. Führen Sie einen der folgenden Schritte aus:
   - Um unsichere LDAP-Verbindungen zuzulassen, aktivieren Sie die Option **Allow Unsecure Connection**.
   - Um LDAP-Verbindungen zu sichern, deaktivieren Sie die Option **Allow Unsecure Connection**.

     Wenn diese Option nicht aktiviert ist, sind alle LDAP-Verbindungen sicher.
6. Geben Sie unter **Administrator Bind DN** den Administrator-Bind-DN für Abfragen ein, die an Ihr LDAP-Verzeichnis gerichtet sind.

   Die Syntax für den Bind-DN kann z. B. wie folgt aussehen:
   Domäne/Benutzername
   „ou=Administrator,dc=ace,dc=com“
   „Benutzer@Domäne.Name“ (für Active Directory)
   „cn=Administrator,cn=Users,dc=ace,dc=com“

   Für Active Directory muss der Gruppenname wie folgt angegeben werden: cn=*Gruppenname*. Der auf dem Access Gateway definierte Gruppenname muss identisch mit dem auf dem LDAP-Server definierten Gruppennamen sein.

   Bei anderen LDAP-Verzeichnissen ist der Gruppenname entweder nicht erforderlich oder er muss, sofern er doch nötig ist, in folgender Form angegeben werden: „ou=*Gruppenname*“.

   Das Access Gateway registriert sich mit den Administratoranmeldeinformationen beim LDAP-Server und sucht dann nach dem Benutzer. Wenn der

Benutzer gefunden ist, hebt das Access Gateway die Registrierung mit den Administratoranmeldeinformationen auf und registriert sich mit den Benutzeranmeldeinformationen erneut.

7. Geben Sie unter **Administrator Password** das Kennwort ein.
8. Geben Sie unter **Base DN (location of users)** den Basis-DN für die Benutzer ein.

   Der Basis-DN wird normalerweise vom Bind-DN abgeleitet, indem der Benutzername entfernt und die Gruppe angegeben wird, in der sich die Benutzer befinden. Die Syntax für den Basis-DN kann z. B. wie folgt aussehen:
   ou=Users,dc=ace,dc=com
   cn=Users,dc=ace,dc=com
9. Geben Sie unter **Server logon name attribute** das Attribut ein, unter dem das Access Gateway nach den Benutzeranmeldenamen für den LDAP-Server suchen soll, den Sie gerade konfigurieren. Das Standardattribut ist **cn**. Bei Verwendung von Active Directory ist das Attribut *cn* einzugeben.
10. Geben Sie unter **Group attribute** den Namen des Attributs ein. Der Standardname lautet „memberOf“. Mit diesem Attribut kann das Access Gateway bei der der Autorisierung die Gruppen abrufen, bei denen der Benutzer Mitglied ist. Klicken Sie auf **Submit**.

Verwenden von Zertifikaten für sichere LDAP-Verbindungen

Für die LDAP-Authentifizierung und -Autorisierung können Sie ein sicheres Clientzertifikat verwenden. Hierfür benötigen Sie eine Zertifizierungsstelle im Unternehmen, z. B. die Zertifikatdienste in Windows Server 2003, die auf demselben Computer wie Active Directory ausgeführt werden. Über die Zertifizierungsstelle können Sie ein Clientzertifikat erstellen.

Für die LDAP-Authentifizierung und -Autorisierung muss das Clientzertifikat sicher sein und SSL verwenden. Sichere Clientzertifikate für LDAP werden auf das Access Gateway hochgeladen.

So laden Sie ein sicheres Clientzertifikat für LDAP hoch:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway und klicken Sie auf die Registerkarte **Administration**.
2. Klicken Sie neben **Upload a .pem private key and client certificate** auf **Browse**.
3. Gehen Sie zum Clientzertifikat und klicken Sie auf **Öffnen**.

Bestimmen der Attribute in Ihrem LDAP-Verzeichnis

Wenn Sie bei der Bestimmung Ihrer LDAP-Verzeichnisattribute Hilfe benötigen, können Sie mit der kostenlos erhältlichen Anwendung LDAP Browser von Softerra ganz einfach nach diesen Attributen suchen.

Laden Sie die kostenlos erhältliche Anwendung LDAP Browser von der Softerra LDAP Administrator-Website (http://www.ldapbrowser.com) herunter. Die Anwendung ist auch mit deutscher Benutzeroberfläche erhältlich. Legen Sie nach der Installation des Browsers folgende Attribute fest:

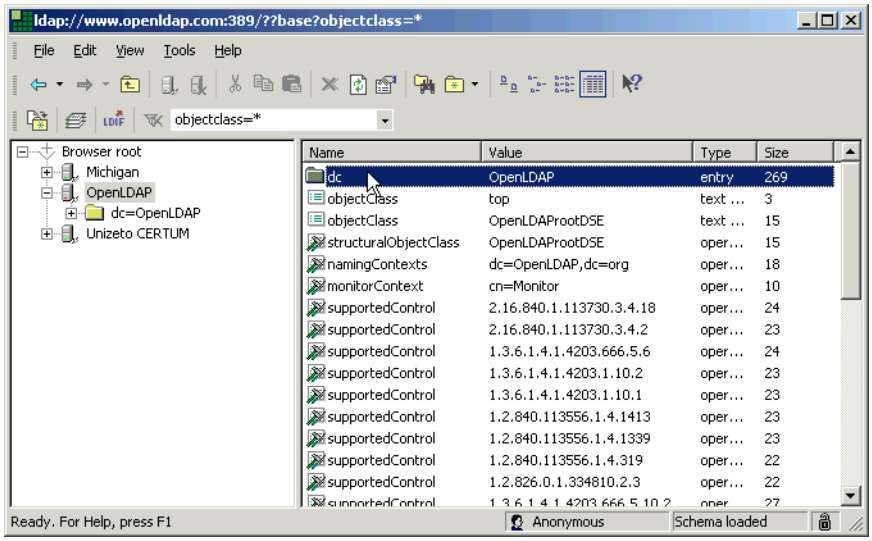
- Hostname oder IP-Adresse Ihres LDAP-Servers.
- Port Ihres LDAP-Servers. Der Standardwert ist 389.
- Das Feld **Base DN** kann leer gelassen werden.

  Anhand der von LDAP Browser bereitgestellten Informationen können Sie den Basis-DN bestimmen, der auf der Registerkarte **Authentication** benötigt wird.
- Mit dem Kontrollkästchen **Anonymous Bind** wird festgelegt, ob der LDAP-Server die Anmeldeinformationen der Benutzer benötigt, um eine Verbindung zum Browser herzustellen. Wenn der LDAP-Server die Anmeldeinformationen benötigt, lassen Sie das Kontrollkästchen deaktiviert.

Wenn alle Einstellungen vorgenommen wurden, zeigt LDAP Browser im linken Bereich den Profilnamen an und stellt eine Verbindung zum LDAP-Server her.

So suchen Sie nach LDAP-Attributen:

1. Wählen Sie im linken Teil von LDAP Browser den Profilnamen aus, den Sie erstellt haben.
2. Wenn Sie den Basis-DN herausfinden möchten, suchen Sie im rechten Teil nach dem Attribut **namingContexts**. Der Wert dieses Attributs ist der Basis-DN für Ihre Site. Der Basis-DN lautet typischerweise wie folgt: dc=Domänenname,dc=com (sofern Ihre Verzeichnisstruktur auf Internetdomänennamen basiert) oder ou=Domäne,o=Organisation,c=Land.



LDAP Browser-Fenster

3. Navigieren Sie in der Anwendung, um auch die anderen Attribute zu finden.

Konfigurieren von RADIUS-Authentifizierung und -Autorisierung

Sie können das Access Gateway für die Authentifizierung des Benutzerzugriffs mit einem oder mehreren RADIUS-Server(n) konfigurieren. Für jeden für die Authentifizierung verwendeten RADIUS-Bereich können Sie einen primären und einen sekundären RADIUS-Server konfigurieren. Wenn der primäre RADIUS-Server nicht verfügbar ist, versucht das Access Gateway, die Authentifizierung für diesen Bereich mit dem sekundären RADIUS-Server vorzunehmen.

Wenn ein Benutzer sich nicht auf den RADIUS-Servern befindet oder wenn die Authentifizierung fehlschlägt, überprüft das Access Gateway den Benutzer anhand der lokal auf dem Access Gateway gespeicherten Benutzerinformationen, sofern auf der Registerkarte **Settings** des Bereichs die Option **Use the local user database on the Access Gateway** aktiviert ist.

Die Access Gateway-Software enthält außerdem die RADIUS-Autorisierung, die mit der RAS-Richtlinie im Microsoft-Internetauthentifizierungsdienst (IAS) konfiguriert wird. Während der Konfiguration des Access Gateways müssen die folgenden Informationen bereitgestellt werden:

- **Vendor Code** (entspricht dem im IAS eingegebenen Herstellercode).
- **Vendor-assigned atttribute number** (entspricht der vom Hersteller zugewiesenen Attributnummer).
- **Attribute Value Prefix** (entspricht dem im IAS definierten Attributwert). Der Standardname lautet **CTXSUserGroups=**.
- Das Trennzeichen (**Separator**) muss angegeben werden, wenn in der RADIUS-Konfiguration mehrere Benutzergruppen enthalten sind. Als Trennzeichen kann ein Leerzeichen, ein Punkt, ein Semikolon oder ein Doppelpunkt verwendet werden.

Wenn der IAS nicht auf dem RADIUS-Server installiert ist, können Sie ihn über **Software** in der Systemsteuerung installieren. Weitere Informationen finden Sie in der Windows-Onlinehilfe.

Zum Konfigurieren des IAS installieren Sie das Snap-In für IAS über die Microsoft Management Console (MMC). Führen Sie den Installationsassistenten aus und wählen Sie dabei die folgenden Einstellungen:

- Wählen Sie **Lokalen Computer**.
- Wählen Sie **RAS-Richtlinien** und erstellen Sie eine benutzerdefinierte Richtlinie.
- Wählen Sie für die Richtlinie **Windows-Groups**.
- Wählen Sie **Verschlüsselte Authentifizierung (CHAP)** und **Unverschlüsselte Authentifizierung (PAP, SPAP)**.
- Wählen Sie nicht **MS-CHAP v2** und **MS-CHAP**.
- Wählen Sie als Attributnamen **Vendor-Specifc** aus.

  Access Gateway benötigt das herstellerspezifische Attribut, um die in der Gruppe auf dem Server definierten Benutzer mit den Benutzern auf dem Access Gateway abzugleichen. Dies erfolgt durch Senden der herstellerspezifischen Attribute an das Access Gateway. Als Hersteller muss **RADIUS Standard** ausgewählt werden.
- Der RADIUS-Standardwert ist 0. Verwenden Sie diesen Wert für den Herstellercode.

- Die vom Hersteller zugewiesene Attributnummer ist 0.

  Dies ist der zugewiesene Wert für das Attribut *CTSXUserGroups*. Das Attribut hat das Format einer Zeichenfolge.

- Wählen Sie als Attributformat **Zeichenfolge** aus.

  Geben Sie unter **Attributwert** den Attributnamen und die Gruppen ein.

  Für das Access Gateway lautet der Attributwert: CTXSUserGroups=*Gruppenname*. Wenn zwei Gruppen definiert sind, z. B. die Gruppen „Vertrieb“ und „Finanzen“, lautet der Attributwert CTXSUserGroups=Vertrieb;Finanzen. Die Gruppen sind dabei jeweils durch ein Semikolon zu trennen.

- Entfernen Sie im Dialogfeld **Einwählprofil bearbeiten** alle anderen Einträge außer dem Eintrag **Vendor-specific**.

Wenn Sie mit dem Konfigurieren der RAS-Richtlinie im IAS fertig sind, gehen Sie zum Access Gateway und konfigurieren Sie die RADIUS-Authentifizierung und -Autorisierung.

So konfigurieren Sie die RADIUS-Authentifizierung:

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie im Feld **Realm name** einen Namen für den Authentifizierungsbereich ein, wählen Sie **One Source** und klicken Sie dann auf **Add**.

Hinweis: Wenn der Bereich **Default** RADIUS-Authentifizierung verwenden soll, entfernen Sie den Bereich **Default** wie unter „So können Sie den Bereich „Default“ entfernen und neu erstellen:“ auf Seite 81 beschrieben.

   Besitzt Ihre Site mehrere Authentifizierungsbereiche, verwenden Sie einen Namen, aus dem deutlich hervorgeht, für welchen RADIUS-Bereich Sie die Einstellungen festlegen. Bei Bereichsnamen ist auf die Groß- und Kleinschreibung zu achten. Darüber hinaus können sie Leerzeichen enthalten.

3. Wählen Sie unter **Authentication type** die Option **RADIUS authentication** und klicken Sie auf **OK**.

   Das Dialogfeld für den Authentifizierungsbereich wird geöffnet.

4. Geben Sie unter **IP Address** die IP-Adresse des RADIUS-Servers ein.
5. Geben Sie im Feld **Port** die Portnummer ein. Die Standardportnummer ist 1812.

6. Geben Sie im Feld **Server secret** den geheimen RADIUS-Schlüssel ein.

   Der geheime Serverschlüssel wird auf dem RADIUS-Server und auf dem Access Gateway manuell konfiguriert.

   Wichtig: Achten Sie darauf, dass der geheime Serverschlüssel stark genug ist. Ein geheimer Schlüssel ist stark, wenn er aus mindestens acht Zeichen besteht und sich aus Buchstaben, Ziffern und Symbolen zusammensetzt.

7. Wenn Sie einen sekundären RADIUS-Server verwenden, geben Sie die IP-Adresse, den Port und den geheimen Schlüssel dieses Servers ein.

RADIUS-Autorisierung

Für die RADIUS-Authentifizierung können Sie die folgenden Autorisierungstypen verwenden:

- RADIUS-Autorisierung
- Lokale Autorisierung
- LDAP-Autorisierung
- Keine Autorisierung

So konfigurieren Sie RADIUS-Autorisierung:

1. Klicken Sie auf die Registerkarte **Authentication** und öffnen Sie den Bereich, für den Sie RADIUS-Autorisierung konfigurieren möchten.
2. Klicken Sie auf die Registerkarte **Authorization** und wählen Sie unter **Authorization type** die Option **RADIUS authorization**.
3. Vervollständigen Sie die Einstellungen mit den im IAS definierten Attributen.
4. Klicken Sie auf **Submit**.

Hinweis: Wenn Sie den Microsoft-Internetauthentifizierungsdienst (IAS) als RADIUS-Server verwenden und beim Senden einer Anforderung an den konfigurierten RADIUS-Server durch das Access Gateway eine Fehlermeldung erhalten, wonach der Benutzername oder das Kennwort ungültig ist, wählen Sie in den IAS-RAS-Richtlinien unter den Eigenschaften für die jeweilige Richtlinie auf der Registerkarte **Authentifizierung** die Option **Unverschlüsselte Authentifizierung (PAP, SPAP)**.

Auswählen der RADIUS-Authentifizierungsprotokolle

Das Access Gateway unterstützt Implementierungen von RADIUS, die für die Verwendung des Password Authentication Protocol (PAP) zur Benutzerauthentifizierung konfiguriert wurden. Andere Authentifizierungsprotokolle, wie Challenge-Handshake Authentication Protocol (CHAP), werden nicht unterstützt.

Wenn Ihre Access Gateway-Bereitstellung für die Verwendung der RADIUS-Authentifizierung und Ihr RADIUS-Server für die Verwendung von PAP konfiguriert ist, können Sie eine stärkere Benutzerauthentifizierung erreichen, indem Sie dem RADIUS-Server einen starken gemeinsamen geheimen Schlüssel zuweisen. Starke gemeinsame geheime RADIUS-Schlüssel bestehen aus willkürlichen Folgen von Groß- und Kleinbuchstaben, Zahlen und Zeichen und sind mindestens 22 Zeichen lang. Verwenden Sie möglichst ein Programm, um die gemeinsamen geheimen RADIUS-Schlüssel zu generieren.

Um den Datenverkehr auf dem RADIUS-Server noch besser zu schützen, können Sie jedem Access Gateway-Gerät einen anderen gemeinsamen geheimen Schlüssel zuweisen. Wenn Sie auf dem RADIUS-Server Clients definieren, können Sie auch jedem Client einen separaten gemeinsamen geheimen Schlüssel zuweisen. Dazu müssen Sie jeden Access Gateway-Bereich, der die RADIUS-Authentifizierung verwendet, einzeln konfigurieren. Wenn Sie die Konfigurationen mehrerer Access Gateway-Geräte in einem Cluster synchronisieren, wird allen Geräten der gleiche geheime Schlüssel zugewiesen.

Gemeinsame geheime Schlüssel werden auf dem Access Gateway konfiguriert, wenn ein RADIUS-Bereich erstellt wird.

Hinweis: Wenn Sie Access Gateway Advanced Edition verwenden, müssen Sie vor der Zuweisung von gemeinsamen geheimen RADIUS-Schlüsseln auf den Servern, auf denen die Advanced Access Control ausgeführt wird und die zum Authentifizieren der Benutzer RADIUS verwenden, ein RADIUS-Authentifizierungsprofil konfigurieren. Weitere Informationen zu Authentifizierungsprofilen finden Sie im *Administratorhandbuch für Access Gateway Advanced Edition*.

Konfigurieren der RSA SecurID-Authentifizierung

Wenn Ihre Site einen RSA ACE/Server und RSA SecurID für die Authentifizierung verwendet, können Sie das Access Gateway für die Authentifizierung des Benutzerzugriffs mit dem RSA ACE/Server konfigurieren. Das Access Gateway agiert dann als RSA-Agenthost, der sich im Namen der Benutzer authentifiziert, die zum Anmelden den Secure Access Client verwenden. Auf dem Access Gateway können mehrere RSA-Bereiche konfiguriert werden. Alle RSA-Bereiche müssen die Datei sdconf.rec verwenden und auf den gleichen RSA ACE/Server verweisen.

Das Access Gateway unterstützt RSA ACE/Server Version 5.2 und höher. Außerdem werden auch Replikationsserver unterstützt. Die Replikationsserverkonfiguration wird auf dem RSA ACE/Server vorgenommen und ist Teil der Datei sdconf.rec, die auf das Access Gateway hochgeladen wird. Wenn dies auf dem RSA ACE/Server konfiguriert ist, versucht das Access Gateway eine Verbindung zu den Replikationsservern herzustellen, falls es zu einem Ausfall oder Verlust der Netzwerkverbindung mit dem primären Server kommt.

Hinweis: Wenn Sie einen RADIUS-Server auf einem RSA-Server ausführen, konfigurieren Sie die RADIUS-Authentifizierung wie unter „Konfigurieren von RADIUS-Authentifizierung und -Autorisierung“ auf Seite 95 beschrieben.

Wenn ein Benutzer sich nicht auf dem RSA ACE/Server befindet oder wenn die Authentifizierung auf diesem Server fehlschlägt, überprüft das Access Gateway den Benutzer anhand der lokal auf dem Access Gateway gespeicherten Benutzerinformationen, sofern auf der Registerkarte **Settings** des Bereichs die Option **Use the local user database on the Access Gateway** aktiviert ist.

Das Access Gateway unterstützt den Next-Token-Modus. Wenn ein Benutzer drei falsche Kennwörter eingibt, fordert der Secure Access Client den Benutzer auf, mit der nächsten Anmeldung so lange zu warten, bis der nächste Tokencode aktiv ist. Der RSA-Server kann so konfiguriert werden, dass das Konto eines Benutzers, der sich zu oft mit einem falschen Kennwort anmeldet, deaktiviert wird.

Für die Kontaktaufnahme mit dem RSA ACE/Server muss das Access Gateway eine Kopie der ACE-Agent-Host-Konfigurationsdatei sdconf.rec enthalten, die vom RSA ACE/Server angelegt wird. Im Folgenden wird beschrieben, wie diese Datei anzulegen und hochzuladen ist.

Hinweis: In den folgenden Schritten werden die unbedingt erforderlichen Einstellungen für das Access Gateway beschrieben. Darüber hinaus können sitespezifische Zusatzeinstellungen vorgenommen werden. Weiterführende Informationen finden Sie in der RSA ACE/Server-Produktdokumentation.

Wenn die Konfiguration des Access Gateways wiederhergestellt werden muss, finden Sie entsprechende Informationen unter „Zurücksetzen des Node Secret“ auf Seite 103.

Wählen Sie beim Erstellen der Datei sdconf.rec die folgenden Einstellungen aus:

- Erstellen Sie einen Agenthost.
- Geben Sie einen beschreibenden Namen für das Access Gateway ein, das als der Agenthost fungiert, für den Sie die Konfigurationsdatei erstellen.
- Verwenden Sie als Netzwerkadresse die interne IP-Adresse des Access Gateways.
- Der Agenttyp ist „UNIX Agent“.
- Stellen Sie sicher, dass bei der Erstellung des Agenthosts die Option **Node Secret Created** auf dem RSA ACE/Server deaktiviert ist. Der RSA ACE/Server sendet das Node Secret zu dem Zeitpunkt an das Access Gateway, zu dem er das erste Mal eine vom Access Gateway stammende Anforderung authentifiziert. Danach ist die Option **Node Secret Created** aktiviert. Durch Deaktivieren der Option und Generieren und Hochladen einer neuen Konfigurationsdatei können Sie den RSA ACE/Server dazu zwingen, ein neues Node Secret an das Access Gateway zu senden.
- Es gibt zwei Möglichkeiten, festzulegen, welche Benutzer sich über das Access Gateway authentifizieren können.
    - Konfigurieren Sie das Access Gateway als offenen Agenthost, der für alle lokal bekannten Benutzer offen ist.
    - Legen Sie die zu authentifizierenden Benutzer fest, indem Sie den Agenthost bearbeiten und die zu aktivierenden Benutzer auswählen.

Nachdem Sie die Einstellungen auf dem RSA-Server vorgenommen haben, erstellen Sie die Datei sdconf.rec. Die von Ihnen erstellte Datei (sdconf.rec) wird auf das Access Gateway hochgeladen.

Weitere Informationen zum Konfigurieren der Einstellungen auf dem RSA-Server finden Sie in der Dokumentation des Herstellers.

So konfigurieren Sie RSA SecurID-Authentifizierung:

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen, der auf den RSA ACE/Server hinweist, ein.
3. Wählen Sie **One Source** und klicken Sie auf **Add**.

Hinweis: Wenn der Bereich **Default** RSA-Authentifizierung verwenden soll, entfernen Sie den Bereich **Default** wie unter „So können Sie den Bereich „Default“ entfernen und neu erstellen:“ auf Seite 81 beschrieben.

---

4. Aktivieren Sie im Dialogfeld **Select Authentication Type** unter **Authentication type** die Option **RSA** SecurID Authentication.
5. Klicken Sie auf **OK**.

   Ein Dialogfeld für den neuen Bereich wird geöffnet.

Achtung: Wenn die auf das Access Gateway hochgeladene Datei sdconf.rec ungültig ist, sendet das Access Gateway u. U. Meldungen an nicht vorhandene IP-Adressen. Netzwerküberwachungseinrichtungen könnten dies als Netzwerkspamming einstufen.

---

6. Klicken Sie zum Hochladen der soeben generierten Datei sdconf.rec auf der Registerkarte **Authentication** auf **Upload sdconf.rec File**, gehen Sie zu der Datei und klicken Sie dann auf **Öffnen**.

   Die Datei sdconf.rec wird normalerweise unter ace\data\config_files und windows\system32 gespeichert.

   - Aus der Dateistatusmeldung geht hervor, ob die Datei sdconf.rec bereits hochgeladen wurde. Wenn dies der Fall ist und Sie diese Datei ersetzen müssen, klicken Sie auf **Upload sdconf.rec File.** Gehen Sie zu der Datei und klicken Sie auf **Öffnen**, um die Datei hochzuladen.
   - Wenn ein Client zum ersten Mal erfolgreich authentifiziert wird, erstellt und speichert der RSA ACE/Server einige Konfigurationsdateien auf dem Access Gateway. Wird anschließend die IP-Adresse des Access Gateways geändert, klicken Sie auf **Remove ACE Configuration Files**, führen Sie nach entsprechender Aufforderung einen Neustart durch und laden Sie dann eine neue Datei sdconf.rec

hoch. Es werden die Dateien sdconf.rec, securid und sdstatus entfernt.

7. Klicken Sie auf **Submit**.

Für die RSA SecureID-Authentifizierung können Sie die folgenden Autorisierungstypen verwenden:

- RSA-Autorisierung
- Lokale Autorisierung
- LDAP-Autorisierung
- Keine Autorisierung

Konfigurieren der RSA-Einstellungen für einen Cluster

Wenn Sie zwei oder mehr Geräte als Cluster konfiguriert haben, muss die Datei sdconf.rec die vollqualifizierten Domänennamen aller Geräte enthalten. Die Datei sdconf.rec wird auf einem Access Gateway installiert und dann veröffentlicht. Dadurch können alle Geräte eine Verbindung zum RSA-Server herstellen.

Sie können auch einschränken, mit welchen Geräten die Benutzer Verbindungen zum RSA-Server herstellen können. Beispiel: Ihr Cluster besteht aus drei Geräten. Wenn die vollqualifizierten Domänennamen des ersten und des zweiten Geräts in der Datei sdconf.rec enthalten sind, der des dritten Geräts aber nicht, können die Benutzer nur mit den ersten beiden Geräten Verbindungen zum RSA-Server herstellen.

Zurücksetzen des Node Secret

Wenn Sie die Konfiguration des Access Gateways mit einer gespeicherten Konfigurationsdatei wiederhergestellt und dabei dieselbe IP-Adresse wie vorher verwendet haben, müssen Sie das Node Secret auf dem RSA ACE/Server zurücksetzen. Da die Konfiguration des Access Gateways wiederhergestellt wurde, gibt es auf dem Access Gateway kein Node Secret mehr, sodass jeder Versuch der Authentifizierung mit dem RSA ACE/Server fehlschlägt.

Nachdem Sie den gemeinsamen geheimen Schlüssel auf dem RSA ACE/Server zurückgesetzt haben, wird der RSA ACE/Server beim nächsten Authentifizierungsversuch aufgefordert, ein Node Secret an das Access Gateway zu senden.

Konfigurieren der Authentifizierung mit Secure Computing SafeWord

Die SafeWord-Produkte bieten sichere Authentifizierung mit tokenbasierten Passcodes. Nach einmaliger Verwendung wird der Passcode von SafeWord sofort ungültig gemacht und kann nicht mehr verwendet werden.

Wenn das Access Gateway das Secure Gateway während einer Secure Gateway- und Webinterface-Bereitstellung ersetzt, können Sie die Authentifizierung auf dem Access Gateway deaktivieren und dem Webinterface weiterhin erlauben, für den eingehenden HTTP-Verkehr die SafeWord-Authentifizierung bereitzustellen. Weitere Informationen zum Konfigurieren des Webinterface finden Sie unter „Bereitstellen von Zugriff auf veröffentlichte Anwendungen“ auf Seite 193.

Das Access Gateway unterstützt SafeWord-Authentifizierung für die folgenden Secure Computing Produkte:

- SafeWord PremierAccess
- SafeWord for Citrix
- SafeWord RemoteAccess

Es gibt mehrere Möglichkeiten, das Access Gateway für die Authentifizierung mit den SafeWord-Produkten von Secure Computing zu konfigurieren:

- Authentifizierung mit einem PremierAccess RADIUS-Server, der zusammen mit SafeWord PremierAccess installiert und für die Authentifizierung zugelassen wird.
- Authentifizierung mit einem SafeWord-IAS-Agent, der eine Komponente von SafeWord RemoteAccess, SafeWord for Citrix und SafeWord PremierAccess 4.0 ist.
- Installation des SafeWord-Webinterface-Agents, der mit dem Citrix Webinterface zusammenarbeitet. Die Authentifizierung muss nicht auf dem Access Gateway konfiguriert werden und kann vom Citrix Webinterface übernommen werden. In dieser Konfiguration werden weder der PremierAccess RADIUS-Server noch der SafeWord-IAS-Agent verwendet.

Konfigurieren der SafeWord-Einstellungen auf dem Access Gateway

Bei der Konfiguration des SafeWord-Servers benötigen Sie folgende Informationen:

- IP-Adresse des Access Gateways. Diese sollte mit der in der Clientkonfiguration des RADIUS-Servers konfigurierten Adresse übereinstimmen.
- Gemeinsamer geheimer Schlüssel. Dieser geheime Schlüssel ist auch auf der Registerkarte **Authentication** auf dem Access Gateway konfiguriert.
- IP-Adresse und Port des SafeWord-Servers.

Konfigurieren Sie einen SafeWord-Bereich zum Authentifizieren der Benutzer. Das Access Gateway agiert als SafeWord-Agent, der im Namen der Benutzer authentifiziert wird, die sich mit dem Secure Access Client angemeldet haben. Wenn ein Benutzer sich nicht auf dem SafeWord-Server befindet oder wenn die Authentifizierung fehlschlägt, überprüft das Access Gateway den Benutzer anhand der lokalen Benutzerliste, sofern die Option **Use the local user database on the Access Gateway** auf der Registerkarte **Settings** aktiviert ist.

Wenn SafeWord als Bereich **Default** verwendet werden soll, entfernen Sie den aktuellen Bereich **Default** und erstellen Sie sofort einen neuen Bereich wie unter „So können Sie den Bereich „Default“ entfernen und neu erstellen:“ auf Seite 81 beschrieben.

So konfigurieren Sie SafeWord auf dem Access Gateway:

1. Klicken Sie im Administration Tool auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen ein.
3. Wählen Sie **One Source** und klicken Sie dann auf **Add**.
4. Wählen Sie unter **Authentication type** die Option **SafeWord authentication** und klicken Sie auf **OK**.

5. Geben Sie unter **Primary SafeWord Server Settings** die folgenden Daten ein:
   - Geben Sie unter **IP address** die IP-Adresse des SafeWord-Servers ein.
   - Geben Sie unter **Port** die Portnummer für den SafeWord RADIUS-Server ein. Der Standardwert ist 1812.

     Dieser Port muss mit der auf dem RADIUS-Server konfigurierten Portnummer übereinstimmen.
   - Geben Sie unter **Server secret** einen gemeinsamen geheimen RADIUS-Schlüssel ein.

     Der gemeinsame geheime Schlüssel muss mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen.
6. Wenn ein zweiter SafeWord-Server vorhanden ist, konfigurieren Sie die Einstellungen unter **Secondary SafeWord Server Settings**.

Konfigurieren der Autorisierung mit SafeWord

Wenn die Authentifizierung mit SafeWord erfolgt, können Sie die folgenden Autorisierungsverfahren verwenden:

- LDAP
- Lokale Benutzerliste
- RADIUS
- Keine Autorisierung

Informationen zum Konfigurieren der LDAP-Autorisierung finden Sie unter „Konfigurieren der LDAP-Autorisierung“ auf Seite 90. Informationen zum Konfigurieren der RADIUS-Autorisierung finden Sie unter „Konfigurieren von RADIUS-Authentifizierung und -Autorisierung“ auf Seite 95.

Durch entsprechende Konfiguration des SafeWord-Servers kann eingestellt werden, dass SafeWord die Gruppenmitgliedschaftsattribute zurückgibt. Weitere Informationen finden Sie in der Produktdokumentation.

Konfigurieren von NTLM-Authentifizierung und -Autorisierung

Das Access Gateway kann so konfiguriert werden, dass Benutzer mit NTLM-Authentifizierung (Windows NT LAN Manager) anhand der Benutzerdatenbank auf einem Windows NT 4.0-Domänencontroller authentifiziert werden.

Wenn ein Benutzer sich nicht in der Benutzerdatenbank auf den Windows NT 4.0-Domänencontrollern befindet oder die Authentifizierung fehlschlägt, kann das Access Gateway den Benutzernamen anhand der lokalen Benutzerliste auf dem Access Gateway überprüfen und den Benutzer anhand der lokalen Liste authentifizieren, sofern das Kontrollkästchen **Use the local user database on the Access Gateway** auf der Registerkarte **Settings** aktiviert ist.

Ein Windows NT 4.0-Domänencontroller unterhält Domänenbenutzerkonten in einer Datenbank auf dem Windows NT 4.0-Server. Ein Domänenbenutzerkonto umfasst einen Benutzernamen und ein Kennwort sowie weitere Informationen über den Benutzer.

Zum Konfigurieren der NTLM-Authentifizierung erstellen Sie einen NTLM-Authentifizierungsbereich, in dem Adresse und Port hinterlegt sind, die das Access Gateway zum Herstellen einer Verbindung zum Windows NT 4.0-Domänencontroller verwendet. Außerdem geben Sie einen Timeoutwert an, mit dem festgelegt wird, in welcher Zeit eine Authentifizierung beim Server abgeschlossen sein muss.

Wenn sich ein Benutzer am Access Gateway anmeldet, gibt er seine Anmeldeinformationen (Benutzername und Kennwort) ein, die im Domänenbenutzerkonto auf dem Windows NT 4.0-Server hinterlegt sind. Das Access Gateway stellt eine Verbindung zum Windows NT 4.0-Server her und übergibt diese Anmeldeinformationen an den Server. Der Server authentifiziert den Benutzer.

So konfigurieren Sie NTLM-Authentifizierung:

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen für den Authentifizierungsbereich ein.

   Wenn Ihre Site mehrere Authentifizierungsbereiche besitzt, sollten Sie einen Namen verwenden, aus dem deutlich der NTLM-Bereich hervorgeht, für den Sie die Einstellungen festlegen. Bei Bereichsnamen ist auf die

Groß- und Kleinschreibung zu achten. Darüber hinaus können sie Leerzeichen enthalten.

Hinweis: Wenn der Bereich **Default** NTLM-Authentifizierung verwenden soll, entfernen Sie den Bereich **Default** wie unter „So können Sie den Bereich „Default“ entfernen und neu erstellen:“ auf Seite 81 beschrieben.

---

3. Wählen Sie **One Source** und klicken Sie auf **Add**.
4. Wählen Sie im Dialogfeld **Select Authentication Type** unter **Authentication type** die Option **NTLM authentication** und klicken Sie auf **OK**.

   Ein Dialogfeld mit dem Namen des neuen Bereichs wird geöffnet.
5. Klicken Sie auf die Registerkarte **Authentication**.
6. Geben Sie im Feld **IP address or FQDN** die IP-Adresse des Windows NT 4.0-Domänencontrollers ein.
7. Geben Sie im Feld **Port** die Nummer des Ports ein, den der Windows NT 4.0-Domänencontroller nach NTLM-Authentifizierungsverbindungen abhört.

   Der Standardport für NTLM-Authentifizierungsverbindungen ist 139.

Hinweis: Wenn als Port 0 (Null) eingegeben wird, versucht das Access Gateway, automatisch eine Portnummer für die Verbindung zu ermitteln.

---

8. Geben Sie im Feld **Time-out (in seconds)** die Zeitspanne in Sekunden ein, innerhalb derer die Authentifizierung abgeschlossen sein muss. Wird die Authentifizierung nicht innerhalb dieses Zeitraums abgeschlossen, schlägt sie fehl.
9. Klicken Sie auf **Submit**.

Konfigurieren der NTLM-Autorisierung

Ein Windows NT 4.0-Domänencontroller unterhält Gruppenkonten. Ein Gruppenkonto besteht aus mehreren Domänenkonten einzelner Benutzer (und anderen Konten).

Zum Konfigurieren der NTLM-Autorisierung klicken Sie im Authentifizierungsbereich auf die Registerkarte **Authorization** und geben die Adresse und den Port ein, den das Access Gateway zum Herstellen einer Verbindung zum Windows NT 4.0-Domänencontroller verwendet. Außerdem geben Sie einen Timeoutwert an, der festlegt, in welcher Zeit eine Autorisierung am Windows NT-Server abgeschlossen sein muss.

Wenn ein Benutzer erfolgreich authentifiziert wurde, gibt der Domänencontroller eine Liste aller globalen Gruppen, denen der authentifizierte Benutzer angehört, an das Access Gateway zurück.

Das Access Gateway prüft dann, ob auf dem Access Gateway ein Benutzergruppenname existiert, der mit einer globalen Windows NT 4.0-Gruppe übereinstimmt, der der Benutzer angehört. Wenn das Access Gateway eine Übereinstimmung findet, erhält der Benutzer die Zugangsrechte zu den internen Netzwerken, die der Benutzergruppe auf dem Access Gateway zugeordnet sind.

So konfigurieren Sie NTLM-Autorisierung:

1. Klicken Sie auf die Registerkarte **Authentication** und öffnen Sie den Bereich, für den Sie NTLM-Autorisierung aktivieren möchten.
2. Klicken Sie auf die Registerkarte **Authorization**.
3. Wählen Sie unter **Authorization type** die Option **NTLM authorization**.
4. Geben Sie im Feld **Server IP Address or FQDN** den vollqualifizierten Domänennamen oder die IP-Adresse des Windows NT 4.0-Domänencontrollers ein, der die NTLM-Autorisierung durchführen wird.
5. Geben Sie im Feld **Server Port** die Portnummer ein.

   Der Standardport für NTLM-Authentifizierungsverbindungen ist 139.

   Hinweis: Wenn als Port 0 (Null) eingegeben wird, versucht das Access Gateway, automatisch eine Portnummer für die Verbindung zu ermitteln.

   ---

6. Geben Sie im Feld **Timeout (in seconds)** die Zeitspanne in Sekunden ein, innerhalb derer die Autorisierung abgeschlossen sein muss, bevor der Authentifizierungsversuch abgebrochen wird.
7. Klicken Sie auf **Submit**.

Konfigurieren von Zweimethodenauthentifizierung

Das Access Gateway unterstützt Zweimethodenauthentifizierung, bei der sich Benutzer mit zwei Authentifizierungstypen anmelden müssen. Sie haben auf der Registerkarte **Authentication** die Möglichkeit, für einen Bereich zwei Authentifizierungsmethoden zu konfigurieren, z. B. LDAP und SafeWord.

Der Bereich **Default** kann für die Zweimethodenauthentifizierung konfiguriert werden. Es können Bereiche mit einer Authentifizierungsmethode und Bereiche mit Zweimethodenauthentifizierung nebeneinander bestehen. So können Sie z. B. einen oder mehrere Bereich(e) für ein einzelnes Authentifizierungsverfahren und zusätzlich einen oder mehrere Bereich(e) einrichten, die für Zweimethodenauthentifizierung konfiguriert sind. In einer gemischten Authentifizierungsumgebung sehen Benutzer bei der Anmeldung zwei Kennwortfelder. Wenn sich Benutzer mit nur einem Authentifizierungstyp anmelden, bleibt das zweite Kennwortfeld leer.

Weitere Informationen zum Anmelden über die Webportalseite finden Sie unter „Anmelden mit Zweimethodenauthentifizierung“ auf Seite 191.

So erstellen und konfigurieren Sie einen Bereich mit Zweimethodenauthentifizierung:

1. Klicken Sie auf die Registerkarte **Authentication**.
2. Geben Sie unter **Add an Authentication Realm** in das Feld **Realm name** einen Namen ein.
3. Wählen Sie **Two Source** und klicken Sie dann auf **Add**.
4. Legen Sie im Dialogfeld **Select Authentication Type** unter **Primary authentication type** und **Secondary authentication type** das jeweilige Authentifizierungsverfahren fest. Klicken Sie auf **OK**.
5. Konfigurieren Sie auf der Registerkarte **Primary Authentication** die Einstellungen für den ersten Authentifizierungstyp und klicken Sie auf **Submit**.
6. Konfigurieren Sie auf der Registerkarte **Secondary Authentication** die Einstellungen für den zweiten Authentifizierungstyp und klicken Sie auf **Submit**.
7. Wählen Sie auf der Registerkarte **Authorization** unter **Authorization type** den gewünschten Autorisierungstyp aus, konfigurieren Sie die Einstellungen und klicken Sie auf **Submit**.

Bei der Zweimethodenauthentifizierung wird die primäre Authentifizierung zuerst überprüft. Ist diese erfolgreich, wird die sekundäre Authentifizierung geprüft. Wenn Sie z. B. auf der Registerkarte **Secondary Authentication** RSA SecurID und auf der Registerkarte **Primary Authentication** LDAP konfiguriert haben, müssen die Benutzer beim Anmelden in das erste Kennwortfeld ihr LDAP-Kennwort und in das zweite Kennwortfeld die RSA SecurID-PIN und den Passcode eingeben. Wenn Benutzer auf **Connect** klicken, nimmt das Access Gateway die Authentifizierung zuerst anhand des LDAP-Kennworts und dann anhand von RSA SecurID-PIN und des Passcode vor.

Ändern der Beschriftung von Kennwortfeldern

Die Beschriftung der Kennwortfelder kann an den Authentifizierungstyp angepasst werden, mit dem sich Benutzer anmelden, damit sie genau wissen, welches Kennwort sie eingeben müssen. Dies ist besonders dann nötig, wenn das Access Gateway für die Unterstützung von Authentifizierungstypen von Drittanbietern konfiguriert ist. Wenn Benutzer sich z. B. mit LDAP und dem starken Authentifizierungssystem Gemalto protiva (RADIUS) authentifizieren müssen, können Sie die Kennwortfelder mit diesen Typen beschriften, damit die Benutzer wissen, was sie eingeben müssen. Statt mit **Kennwort** und **Sekundäres Kennwort** könnten die Felder z. B. mit **Windows-Domänenkennwort** und **Gemalto protiva-Passcode** beschriftet werden. Die Beschriftungen können je nach Verwendung einzelner Authentifizierungsmethoden oder Zweimethodenauthentifizierung geändert werden.

So ändern Sie die Beschriftungen der Kennwortfelder:

1. Klicken Sie auf die Registerkarte **Authentication** und unter **Add an Authentication Realm** auf **Advanced**.
2. Geben Sie in den Feldern **Password label** und **Secondary password label** die Beschriftungen für die Felder ein.
3. Klicken Sie auf **OK**.

Wenn sich Benutzer anschließend anmelden, sehen sie die neuen Feldbeschriftungen.

KAPITEL 7

Konfigurieren von Netzwerkzugriff und Gruppenressourcen

Benutzer greifen über das Netzwerk auf Unternehmensressourcen zu. Sie können Zugriff auf beliebige Subnetze Ihres Netzwerks gewähren oder verweigern. Beispiel: Sie können einem Benutzer Zugriff auf eine Dateifreigabe auf Ihrem Netzwerk gewähren oder dem Benutzer vollen Zugriff auf alle Ressourcen im Netzwerk geben. Wenn Sie Netzwerkzugriff und Gruppenressourcen konfigurieren, erstellen Sie Zugriffssteuerungslisten. Basierend auf diesen Listen können Sie steuern, auf welche Ressourcen Benutzer zugreifen können, wenn Sie eine Verbindung zum Unternehmensnetzwerk herstellen.

In diesem Kapitel wird die Konfiguration von Netzwerkrichtlinien erläutert, die Benutzern den Zugriff auf das sichere Netzwerk ermöglichen. Unter anderem werden folgende Themen behandelt:

- Konfigurieren des Netzwerkrouting
- Bereitstellen von Netzwerkzugriff für Benutzer
- Aktivieren von Split-Tunneling und zugänglichen Netzwerken
- Konfigurieren von Benutzergruppen
- Konfigurieren von Ressourcen für eine Benutzergruppe
- Konfigurieren von Netzwerkressourcen
- Festlegen von Anwendungsrichtlinien
- Konfigurieren von Endpunktrichtlinien und -ressourcen

Konfigurieren des Netzwerkrouting

Um Zugriff auf interne Netzwerkressourcen zu gewähren, muss das Access Gateway in der Lage sein, Daten an interne Netzwerke weiterzuleiten.

Die Netzwerke, an die das Access Gateway Daten weiterleiten kann, werden durch die Konfiguration der Access Gateway-Routingtabelle und das für das Access Gateway festgelegte Standardgateway bestimmt.

Wenn das Access Gateway ein Paket erhält, überprüft es die Routingtabelle. Wenn sich die Zieladresse des Pakets in einem Netzwerk befindet, für das eine Route in der Routingtabelle vorhanden ist, wird das Paket an dieses Netzwerk weitergeleitet.

Wenn das Access Gateway ein Paket erhält und die Routingtabelle keine Route für die Zieladresse des Pakets enthält, sendet das Access Gateway das Paket an das Standardgateway. Die Routingfunktionen des Standardgateways bestimmen dann, wie das Paket weitergeleitet wird.

Die Routingtabelle des Access Gateways muss alle Routen enthalten, die zum Weiterleiten von Daten an interne Netzwerkressourcen erforderlich sind, auf die Benutzer eventuell Zugriff benötigen.

Sie legen fest, wie die Access Gateway-Routingtabelle konfiguriert werden. Sie können eine Routing Information Protocol (RIP)-Option auswählen, sodass Routen von einem RIP-Server automatisch konfiguriert werden, oder Sie können eine statische Routingoption auswählen und die Routen manuell konfigurieren. Weitere Informationen hierzu finden Sie unter „Konfigurieren von dynamischen und statischen Routen“ auf Seite 64.

Bereitstellen von Netzwerkzugriff für Benutzer

Die Netzwerkressourcen, zu denen Sie Benutzern Zugriff gewähren, müssen sich in einem Netzwerk befinden, an das das Access Gateway Daten weiterleiten kann. Sie können das Access Gateway so konfigurieren, dass entweder dynamische oder statische Routen zum Weiterleiten von Daten an interne Netzwerkressourcen verwendet werden.

Sie können mit dem Access Gateway ganz gezielt festlegen, wie Sie Benutzern Zugriff auf Netzwerkressourcen gewähren. Der Benutzerzugriff auf Netzwerkressourcen lässt sich folgendermaßen steuern:

- Sie erstellen Netzwerkressourcengruppen.

  Eine Netzwerkressourcengruppe enthält einen oder mehrere Netzwerkstandort(e). Im Allgemeinen ist eine Netzwerkressourcengruppe eine Teilgruppe aller Netzwerkressourcen, an die das Access Gateway Daten weiterleiten kann.

So kann eine Ressourcengruppe z. B. den Zugriff auf eine einzelne Anwendung, eine Gruppe von Anwendungen, einen Bereich von IP-Adressen oder das gesamte Intranet ermöglichen. Welche Elemente Sie in eine Netzwerkressourcengruppe aufnehmen, hängt in hohem Maße von den verschiedenen Zugriffsanforderungen Ihrer Benutzer ab. So kann es sein, dass Sie einigen Benutzergruppen Zugriff auf viele Ressourcen gewähren möchten, während andere Benutzergruppen lediglich auf einen kleinen Teilsatz der Ressourcen zugreifen können sollen. Durch Erlauben und Verweigern des Benutzergruppenzugriffs auf Netzwerkressourcengruppen erstellen Sie eine Zugriffssteuerungsliste (Access Control List, ACL) für die betreffende Benutzergruppe.

- Sie bestimmen, ob eine Benutzergruppe ohne eine ACL vollen Zugriff auf Ressourcen in einem Netzwerk hat, an das das Access Gateway Daten weiterleiten kann.

  Standardmäßig haben Benutzergruppen ohne ACL Zugriff auf alle Ressourcen in allen Netzwerken, an die das Access Gateway Daten weiterleiten kann. Dieses Standardverhalten empfiehlt sich, wenn die meisten Ihrer Benutzergruppen vollen Netzwerkzugriff haben sollen. Bei Beibehaltung dieses Standardverhaltens müssen Sie eine Zugriffssteuerungsliste nur für die Benutzergruppen konfigurieren, die keinen vollen Netzwerkzugriff haben sollen. Das Standardverhalten kann auch für einen ersten Test der Bereitstellung nützlich sein.

  Sie können das Standardverhalten ändern, sodass Benutzergruppen der Netzwerkzugriff so lange verweigert wird, bis sie ausdrücklich berechtigt sind, auf eine oder mehrere Netzwerkressourcengruppen zuzugreifen.

- Sie konfigurieren Zugriffssteuerungslisten für Benutzergruppen, indem Sie festlegen, welche Netzwerkressourcen für die einzelnen Benutzergruppen zugänglich oder nicht zugänglich sein sollen.

  Standardmäßig ist der Zugriff auf alle Netzwerkressourcengruppen erlaubt und der Netzwerkzugriff wird durch die Option **Deny Access without access control list (ACL)** auf der Registerkarte **Global Cluster Policies** gesteuert. Wenn Sie den Zugriff auf eine Ressourcengruppe erlauben oder verweigern, wird automatisch auch der Zugriff auf alle anderen Ressourcengruppen verweigert und der Netzwerkzugriff für die Benutzergruppe wird ausschließlich über deren Zugriffssteuerungsliste gesteuert.

  Wenn eine Ressourcengruppe eine Ressource enthält, auf die eine Benutzergruppe keinen Zugriff haben soll, können Sie eine separate Ressourcengruppe nur für diese Ressource erstellen und der Benutzergruppe den Zugriff auf diese spezifische Ressource verweigern.

Die folgende Tabelle enthält eine Zusammenfassung der soeben beschriebenen Optionen.

ACL vorhanden für Benutzer-gruppen?	Zugriff verweigern ohne ACL?	Für die Benutzergruppe zugängliche Ressourcen
Nein	Nein	Beliebiges Netzwerk, auf das das Access Gateway zugreifen kann
Ja	Nein	erlaubte Ressourcengruppen
Nein	Ja	Kein Zugriff auf das Netzwerk
Ja	Ja	erlaubte Ressourcengruppen

Bei der Konfiguration des Netzwerkzugriffs muss die strengste Richtlinie als erste und die schwächste Richtlinie als letzte konfiguriert werden. Beispiel: Sie möchten Zugriff auf alle Ressourcen im Netzwerk 10.0.x.x gewähren, aber Zugriff auf Netzwerk 10.0.20.x verweigern. Konfigurieren Sie als erstes Zugriff auf das Netzwerk 10.0.20.x und dann auf das Netzwerk 10.0.x.x.

Aktivieren von Split-Tunneling und zugänglichen Netzwerken

Auf der Registerkarte **Global Cluster Policies** können Sie *Split-Tunneling* aktivieren, um zu verhindern, dass der Secure Access Client unnötige Netzwerkdaten an das Access Gateway sendet.

Wenn Split-Tunneling nicht aktiviert ist, empfängt der Secure Access Client den gesamten vom Clientcomputer ausgehenden Datenverkehr und leitet ihn durch den VPN-Tunnel an das Access Gateway weiter.

Wenn Sie Split-Tunneling aktivieren, sendet der Secure Access Client nur solche Daten durch den VPN-Tunnel, die für durch das Access Gateway geschützte Netzwerke bestimmt sind. Der Secure Access Client sendet keine Daten, die für ungeschützte Netzwerke bestimmt sind, an das Access Gateway.

Wenn Sie Split-Tunneling aktivieren, müssen Sie eine Liste zugänglicher Netzwerke auf der Registerkarte **Global Cluster Policies** angeben. Die Liste der zugänglichen Netzwerke muss alle internen Netzwerke und Subnetzwerke enthalten, auf die der Benutzer eventuell mit dem Secure Access Client zugreifen muss.

Der Secure Access Client verwendet die Liste der zugänglichen Netzwerke als Filter, um zu bestimmen, ob vom Clientcomputer gesendete Pakete an das Access Gateway gesendet werden sollen.

Beim Start des Secure Access Clients erhält er die Liste zugänglicher Netzwerke vom Access Gateway. Der Secure Access Client überprüft alle vom Clientcomputer übertragenen Pakete und vergleicht die Adressen in den Paketen mit der Liste der zugänglichen Netzwerke. Wenn die Zieladresse im Paket sich in einem der zugänglichen Netzwerke befindet, sendet der Secure Access Client das Paket durch den VPN-Tunnel an das Access Gateway. Befindet sich die Zieladresse nicht in einem zugänglichen Netzwerk, wird das Paket nicht verschlüsselt und der Client leitet das Paket dementsprechend weiter.

Hinweis: Wenn Benutzer mit Citrix Presentation Server Clients eine Verbindung zu in der Serverfarm veröffentlichten Anwendungen herstellen, muss Split-Tunneling nicht aktiviert werden.

So aktivieren Sie Split-Tunneling und zugängliche Netzwerke:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Aktivieren Sie im Bereich **Access options** die Option **Enable split tunneling**.
3. Geben Sie im Feld **Accessible networks** die Liste der Netzwerke ein, die Netzwerkressourcen enthalten, auf die Benutzer mit dem Secure Access Client zugreifen müssen. Trennen Sie dabei die einzelnen Netzwerkeinträge durch ein Leerzeichen oder einen Zeilenumbruch voneinander.
4. Klicken Sie auf **Submit**.

Konfigurieren von Benutzergruppen

Benutzergruppen definieren die Ressourcen, auf die der Benutzer zugreifen darf, wenn er über das Access Gateway eine Verbindung zum Unternehmensnetzwerk herstellt. Gruppen sind mit der Liste der lokalen Benutzer verknüpft. Nach dem Hinzufügen lokaler Benutzer zu einer Gruppe können Sie auf der Registerkarte **Access Policy Manager** die Ressourcen definieren, auf die diese Benutzer Zugriff haben sollen. Weitere Informationen zum Konfigurieren von lokaler Benutzer finden Sie unter „Konfigurieren lokaler Benutzer“ auf Seite 84.

Wenn Sie die Autorisierung auf dem Access Gateway aktivieren, werden die Benutzergruppeninformationen nach dem Authentifizieren des Benutzers vom Authentifizierungsserver abgerufen. Wenn der vom Authentifizierungsserver abgerufene Gruppenname mit einem lokal auf dem Access Gateway erstellten Gruppennamen übereinstimmt, werden die Eigenschaften der lokalen Gruppe für die vom Authentifizierungsserver abgerufene Gruppe verwendet.

Wichtig: Die Gruppennamen auf den Authentifizierungsservern und auf dem Access Gateway müssen identisch sein (auch hinsichtlich der Groß- und Kleinschreibung).

Konfigurieren von Zugriffssteuerungslisten

Jeder Benutzer sollte mindestens einer Gruppe angehören, die lokal auf dem Access Gateway definiert ist. Wenn ein Benutzer keiner Gruppe angehört, wird anhand von Zugriffssteuerungslisten bestimmt, auf welche Ressourcen der Benutzer Zugriff hat. Diese Zugriffssteuerungslisten können mit der Option **Deny access without access control list (ACL)** folgendermaßen angepasst werden:

- Wenn die Option **Deny Access** aktiviert ist, kann der Benutzer keine Verbindung herstellen.
- Wenn die Option **Deny Access** deaktiviert ist, hat der Benutzer vollen Zugriff auf das Netzwerk.
- In beiden Fällen kann der Benutzer zwar den Kioskmodus verwenden, aber der Netzwerkzugriff innerhalb dieser Sitzung richtet sich nach der Einstellung für **Deny access without access control list (ACL)**.

So verweigern Sie Benutzergruppen ohne Zugriffssteuerungsliste den Zugriff:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Klicken Sie im Bereich **Access Options** auf **Deny access without access control list (ACL)**.
3. Klicken Sie auf **Submit**.

Erstellen lokaler Benutzergruppen

Sie können auch lokale Gruppen hinzufügen, die in keiner Beziehung zu Gruppen auf den Authentifizierungsservern stehen. So können Sie z. B. eine lokale Gruppe erstellen, um einen Vertragspartner oder Besucher einzurichten, der vorübergehend Zugriff haben soll. Das Erstellen eines Eintrags auf dem Authentifizierungsserver ist dabei nicht nötig. Informationen zum Erstellen eines lokalen Benutzers finden Sie unter „Konfigurieren lokaler Benutzer“ auf Seite 84.

Hinweis: Wenn Sie eine Benutzergruppe mit mehr als 127 Zeichen erstellen und diese Gruppe anschließend löschen, wird sie dennoch weiterhin auf der Registerkarte **Group Priority** angezeigt. Sie können dieses Problem umgehen, indem Sie Benutzergruppennamen mit weniger als 127 Zeichen verwenden. Alle Zeichen, die diese Grenze überschreiten, werden abgeschnitten.

Konfigurieren von Ressourcengruppen

Eine Reihe von Aspekten des Access Gateway-Betriebs werden auf Gruppenebene konfiguriert. Dabei wird zwischen Gruppeneigenschaften und Gruppenressourcen unterschieden.

Zu den Gruppeneigenschaften gehören Folgende:

- Gruppen, die die Eigenschaften der Standardgruppe übernehmen.
- Erzwingen einer erneuten Anmeldung durch die Benutzer, wenn es zu einer Netzwerkunterbrechung gekommen ist oder wenn sich der Computer im Standby-Modus oder Ruhezustand befunden hat.
- Aktivieren der Single Sign-On-Funktionalität unter Windows.
- Aktivieren von Single Sign-On für das Webinterface.
- Ausführen von Anmeldeskripten, wenn ein Benutzer sich mit Domänenanmeldeinformationen anmeldet.
- Verweigern des Zugriffs auf Anwendungen in dem Netzwerk, das keine definierte Anwendungsrichtlinie besitzt.
- Deaktivieren der Desktopfreigabefunktion des Secure Access Clients.
- Zugriffskonfiguration zum Festlegen der Zeitdauer für eine Sitzung. Es gibt drei Arten von Sitzungstimeouts:

  - Benutzersitzungstimeout: Hiermit wird festgelegt, wie lange ein Benutzer angemeldet bleiben kann, unabhängig davon ob Aktivität stattfindet. Die angegebene Zeit ist absolut. Wenn für den Benutzer ein Timeout von 60 Minuten festgelegt ist, endet die Sitzung nach 60 Minuten. 1 Minute vorher werden die Benutzer in einer Warnmeldung auf das nahende Sitzungsende hingewiesen.
  - Netzwerkaktivitätstimeout: Hierbei wird der Benutzer nach einer bestimmten Zeitspanne abgemeldet, wenn keine Netzwerkaktivität vom Clientgerät durch den VPN-Tunnel festgestellt wurde. Netzwerkaktivität vom LAN wird nicht berücksichtigt.
  - Timeout bei inaktiver Sitzung: Hierbei wird Netzwerkaktivität festgestellt, aber keine Benutzeraktivität. Benutzeraktivitäten sind Tastatureingaben oder Mausbewegungen.
- Aktivieren von Split DNS, sodass der Client nur die Daten durch den VPN-Tunnel sendet, die an das sichere Netzwerk gerichtet sind.
- IP-Pooling, wenn jedem Client eine eindeutige IP-Adresse zugewiesen ist.
- Anmelde- und Portalseitenverwendung, womit definiert wird, welche Seite dem Benutzer bei der Anmeldung angezeigt wird. Die Anmeldeseite kann entweder eine von Citrix bereitgestellte Seite oder eine auf das einzelne Unternehmen zugeschnittene Seite sein. Wenn Ihr Unternehmen Citrix Presentation Server verwendet, kann die Anmeldeseite das Webinterface sein. Wenn Sie dem Benutzer mehrere Optionen zur Anmeldung geben möchten, verwenden Sie die Seite mit mehreren Anmeldeoptionen. Weitere Informationen hierzu finden Sie unter „Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen“ auf Seite 190.
- Erzwingen von Clientzertifikaten.

Zu den Gruppenressourcen gehören:

- Netzwerkressourcen, die die Netzwerke definieren, zu denen die Clients eine Verbindung herstellen können.
- Anwendungsrichtlinien, die die Anwendungen definieren, die die Benutzer bei Herstellung einer Verbindung verwenden können. Neben dem Auswählen der Anwendung können Sie auch definieren, auf welche Netzwerke die Anwendung zugreifen kann und ob beim Herstellen einer Verbindung Endpunktrichtlinien erfüllt werden müssen.
- Dateifreigaberessourcen, die definieren, zu welchen Dateifreigaben der Benutzer bei Anmeldung im Kioskmodus eine Verbindung herstellen kann.
- Kioskressourcen, die definieren, wie sich der Benutzer anmelden kann und auf welche Dateifreigaben und Anwendungen der Benutzer zugreifen kann,

während er angemeldet ist. Wenn der Benutzer den Firefox-Webbrowser im Kioskmodus verwenden darf, ist auch die Webadresse, die der Benutzer verwenden darf, definiert.

- Endpunktressourcen und -richtlinien, die die erforderlichen und die optionalen Parameter definieren, die auf dem Computer des Benutzers beim Anmelden vorhanden sein müssen.

Wenn ein Benutzer zu mehreren Gruppen gehört, gelten für diesen Benutzer bestimmte Gruppenrichtlinien, deren Anwendung sich nach den auf der Registerkarte **Group Priority** festgelegten Gruppenprioritäten richtet. Informationen zum Festlegen der Gruppenprioritäten finden Sie unter „Festlegen der Priorität von Gruppen“ auf Seite 135.

Erstellen von Benutzergruppen

Benutzergruppen werden auf der Registerkarte **Access Policy Manager** erstellt. Es ist möglich, mehrere Benutzergruppen zu erstellen und zu konfigurieren. Beim Erstellen einer neuen Gruppe wird die Eigenschaftenseite angezeigt, auf der Sie die Einstellungen für die Gruppe konfigurieren können. Wenn alle Einstellungen festgelegt sind, können der Gruppe Ressourcen hinzugefügt werden.

So erstellen Sie eine lokale Benutzergruppe auf dem Access Gateway:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **User Groups** und klicken Sie dann auf **New Group**.

   Geben Sie unter **Group Name** einen aussagekräftigen Namen für die Gruppe ein (z. B. „Temp. Mitarbeiter“ oder „Buchhaltung“) und klicken Sie dann auf **OK**.

   Wichtig: Wenn die Eigenschaften der Gruppe für die Authentifizierung mittels Authentifizierungsservern verwendet werden sollen, muss der Gruppenname mit dem Gruppennamen auf dem Authentifizierungsserver identisch sein (auch hinsichtlich der Groß- und Kleinschreibung und der verwendeten Leerzeichen).

   Ein Dialogfeld für die hinzugefügte Gruppe wird geöffnet.
3. Informationen zum Konfigurieren der Gruppe finden Sie unter „Konfigurieren von Ressourcen für eine Benutzergruppe“ auf Seite 123.

So entfernen Sie eine Benutzergruppe:

Klicken Sie mit der rechten Maustaste im linken Bereich der Registerkarte **Access Policy Manager** auf eine Gruppe und klicken Sie dann auf **Delete**.

Eigenschaften der Standardgruppe („Default“)

Wenn die einzige auf dem Access Gateway konfigurierte Gruppe die Standardbenutzergruppe ist, erhalten alle lokalen Benutzer die für diese Gruppe konfigurierten Einstellungen. Sie können den Zugriff einschränken, indem Sie zusätzliche Gruppen auf dem Access Gateway konfigurieren und dann entscheiden, ob sie denselben Zugriff wie die Standardbenutzergruppe erhalten sollen.

Beispiel: Zwei Benutzer gehören einer Gruppe temporärer Mitarbeiter an. Sie dürfen Verbindungen zu bestimmten Unternehmensressourcen, z. B. einem Exchange-Server und einem Dateiserver, herstellen. Wenn sie die Einstellungen der Standardgruppe erben, erhalten sie dadurch unter Umständen Zugriff auf Ressourcen, die nur für festangestellte Mitarbeiter bestimmt sind.

In den Benutzergruppeneigenschaften können Sie festlegen, ob Benutzer die Einstellungen der Standardgruppe erben sollen. Für die Standardgruppe ist diese Option nicht verfügbar.

So aktivieren oder deaktivieren Sie die Eigenschaften der Gruppe „Default“:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf die Benutzergruppe und klicken Sie dann auf **Properties**.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn die Benutzer die Einstellungen der Standardgruppe nicht erben sollen, deaktivieren Sie die Option **Inherit properties from the Default group**.
   - Wenn die Benutzer die Einstellungen der Standardgruppe erben sollen, aktivieren Sie die Option **Inherit properties from the Default group**.
4. Klicken Sie auf **OK**.

Konfigurieren von Ressourcen für eine Benutzergruppe

Ressourcen für Benutzergruppen werden im rechten Bereich der Registerkarte **Access Policy Manager** konfiguriert. Zu den Ressourcen gehören:

- Network Resources (Netzwerkressourcen)
- Application Policies (Anwendungsrichtlinien)
- File Share Resources (Dateifreigaberessourcen)
- Kiosk Resources (Kioskressourcen)
- End Point Resources (Endpunktressourcen)
- End Point Policies (Endpunktrichtlinien)
- Pre-Authentication Policies (Vorauthentifizierungsrichtlinien)

Nachdem Sie die Einstellungen konfiguriert haben, ziehen Sie die Ressource auf die Gruppe im linken Bereich. Beispiel: Sie haben eine Netzwerkressource konfiguriert und gespeichert, in der die Netzwerke angegeben sind, zu denen die Benutzer eine Verbindung herstellen können. Wenn Sie eine Gruppe von temporären Mitarbeitern haben, für die nur eingeschränkte Rechte gelten, ziehen Sie die Ressource auf diese Gruppe und legen Sie dann für die Gruppe fest, dass sie nicht die Einstellungen der Standardgruppe erben soll.

Sie können für jede Benutzergruppe eine Zugriffssteuerungsliste (ACL) erstellen, indem Sie wie unter „Bereitstellen von Netzwerkzugriff für Benutzer“ auf Seite 114 beschrieben die Ressourcen festlegen, auf die die jeweilige Gruppe zugreifen darf. Die Zugriffssteuerungslisten werden für alle Gruppen, denen die Benutzer angehören, kombiniert und dann auf die Benutzer angewendet.

Sofern nicht alle Benutzer vollen Zugriff auf alle zugänglichen Netzwerke haben sollen, müssen Sie die Benutzergruppen mit Ressourcengruppen verknüpfen.

Konfigurieren von Benutzern, die mehreren Gruppen angehören

Wenn ein Benutzer Mitglied mehrerer Gruppen ist, werden einige Gruppeneinstellungen *zusammengefasst*. Dabei handelt es sich um folgende Einstellungen:

- Network Resources
- Application Policies
- Kiosk Resources
- End Point Policies

Für die zusammengefassten Einstellungen gelten folgende Ausnahmen:

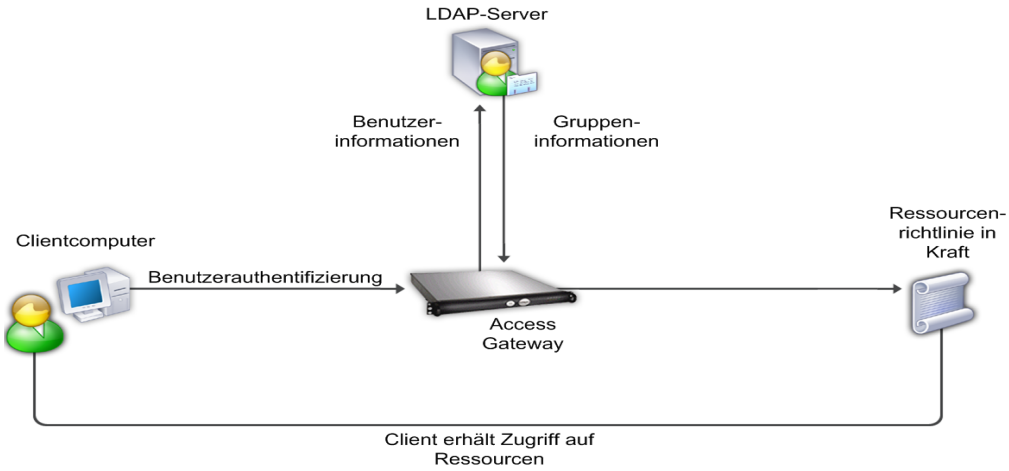
- Deny applications without policies: Wenn für eine der Gruppen, zu denen ein Benutzer gehört, die Option **Deny applications without policies** aktiviert ist, gilt diese Einstellung auch für den Benutzer.
- Enable IP pools: Die Benutzer übernehmen die IP-Adresse von der Gruppe mit der höchsten Priorität, für die IP-Pools aktiviert sind.
- Inherit properties from the Default Group: Wenn für eine der Gruppen, zu denen ein Benutzer gehört, die Option **Inherit properties from the Default Group** aktiviert ist, erbt der Benutzer die Einstellungen der Standardgruppe.

Die Einstellungen, die nicht zusammengefasst werden, richten sich nach der Gruppenpriorität. Dazu gehören folgende Einstellungen:

- Authenticate after network interruption/Authenticate upon system resume
- Enable single sign-on with Windows
- Run logon scripts
- Session timeout
- Enable split DNS
- Enable logon page authentication

Konfigurieren von Netzwerkressourcen

Netzwerkressourcen definieren die Speicherorte auf dem Unternehmensnetzwerk, auf die autorisierte Benutzer zugreifen können. Ressourcengruppen sind mit Benutzergruppen verknüpft, um so Richtlinien für die Ressourcenzugriffssteuerung zu bilden.



Netzwerktopologie für Ressourcengruppen und Authentifizierung

Stellen Sie sich vor, Sie möchten einer Benutzergruppe den sicheren Zugriff auf Folgendes bereitstellen:

- Subnetz 10.10.x.x
- Subnetz 10.20.10.x
- IP-Adressen 10.50.0.60 und 10.60.0.10

Erstellen Sie zu diesem Zweck eine Netzwerkressourcengruppe, indem Sie das folgende Paar aus IP-Adresse und Subnetzmaske festlegen:

```
10.10.0.0/255.255.0.0
10.20.10.0/255.255.255.0
10.50.0.60/255.255.255.255
10.60.0.10/255.255.255.255
```

Die Subnetzmaske können Sie in der CIDR-Notation (Classless Inter Domain Routing) angeben. Beispiel: Sie könnten 10.60.0.10/32 als letzten Eintrag festlegen.

Beachten Sie beim Arbeiten mit Ressourcengruppen darüber hinaus die folgenden Hinweise.

- Sie können den Zugriff zusätzlich einschränken, indem Sie für ein Paar aus IP-Adresse und Subnetzmaske einen Port, einen Portbereich und ein Protokoll angeben. So könnten Sie z. B. festlegen, dass eine Ressource nur Port 80 und das TCP-Protokoll verwenden kann.
- Beim Konfigurieren des Ressourcengruppenzugriffs für eine Benutzergruppe können Sie den Zugriff auf jede Ressourcengruppe zulassen oder verweigern. Auf diese Weise können Sie einen Teil einer ansonsten zugelassenen Ressource ausschließen. So können Sie z. B. einer Benutzergruppe den Zugriff auf 10.20.10.0/24 erlauben, während Sie aber den Zugriff auf 10.20.10.30 verweigern. Verweigerungsregeln besitzen eine höhere Priorität als Zulassungsregeln.
- Die einfachste Methode, allen Benutzergruppen den Zugriff auf alle Netzwerkressourcen bereitzustellen, besteht darin, überhaupt keine Ressourcengruppen zu erstellen und die Option **Deny access without access control list (ACL)** auf der Registerkarte **Global Cluster Policies** zu deaktivieren. Alle Benutzergruppen haben dann Zugriff auf alle Netzwerkressourcen, auf die über das Access Gateway zugegriffen werden kann.
- Wenn Sie Benutzergruppen haben, die Zugriff auf alle Netzwerkressourcen benötigen, erstellen Sie eine Ressourcengruppe für 0.0.0.0/0.0.0.0 und geben Sie den Benutzergruppen Zugriff auf diese Ressource. Für alle anderen Benutzergruppen können Sie die einzelnen Ressourcengruppen nach Bedarf zulassen oder verweigern.

So erstellen und konfigurieren Sie eine Netzwerkressource:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **Network Resources** und klicken Sie dann auf **New Network Resource**.
3. Geben Sie einen Namen für die Gruppe ein und klicken Sie auf **OK**.
4. Geben Sie unter **Network and subnet mask** das Paar aus IP-Adresse und Subnetzmaske für die Ressource ein. Sie können für die Subnetzmaske die CIDR-Notation verwenden. Trennen Sie die einzelnen Einträge durch ein Leerzeichen voneinander.

5. Geben Sie unter **Port or port range** die Ports ein, über die das Access Gateway Verbindungen zu den Netzwerkressourcen herstellen kann. Sie haben folgende Optionen:

   - Geben Sie eine 0 (Null) ein, um alle Ports zu verwenden.
   - Geben Sie einen einzelnen Port ein oder mehrere Ports, die nicht in einem Bereich unmittelbar aufeinander folgen. Wenn Sie mehrere Ports eingeben, trennen Sie sie durch ein Komma. Beispiel: Wenn Sie Verbindungen über die Ports 22, 80 und 8088 zulassen möchten, geben Sie Folgendes ein:

     22, 80, 8080
   - Geben Sie einen Portbereich ein. Trennen Sie den ersten Port in der Reihenfolge mit einem Bindestrich (-) vom letzten Port des Bereichs. Beispiel: Wenn Sie Verbindungen über alle Ports von 110 bis 120 zulassen möchten, geben Sie Folgendes ein:

     110-120
   - Sie können auch eine Kombination aus einzelnen Ports und Portbereichen eingeben. Beispiel: Wenn Sie Verbindungen über die Ports 22, 80, 8088 und 110 bis 120 zulassen möchten, geben Sie Folgendes ein:

     22, 80, 8080, 110-120
6. Wählen Sie unter **Protocol** die Protokolle aus, mit denen Verbindungen auf den angegebenen Ports hergestellt werden können.
7. Klicken Sie auf **OK**.

So fügen Sie einer Gruppe eine Netzwerkressource hinzu:

Klicken Sie auf der Registerkarte **Access Policy Manager** im rechten Bereich unter **Network Resources** auf die Ressource, die Sie hinzufügen möchten, und ziehen Sie sie auf die Benutzergruppe im linken Bereich.

Zulassen und Verweigern von Netzwerkressourcen und Anwendungsrichtlinien

Standardmäßig sind alle Netzwerkressourcen und Anwendungsrichtlinien zugelassen. Wenn der Zugriff auf eine Ressourcengruppe verweigert wird, wird automatisch auch der Zugriff auf alle anderen Ressourcengruppen verweigert und der Netzwerkzugriff für die Benutzergruppe wird nur über deren Zugriffssteuerungsliste gesteuert.

Das Access Gateway interpretiert „Zulassen“ und „Verweigern“ wie folgt:

- Das Access Gateway verweigert den Zugriff auf alle Netzwerkressourcen oder Anwendungsrichtlinien, die nicht explizit zugelassen sind. Wenn Sie einer bestimmten Benutzergruppe also den Zugriff auf nur eine Ressourcengruppe erlauben möchten, gestatten Sie ihr auch nur den Zugriff auf diese bestimmte Ressourcengruppe.
- Verweigerungsregeln besitzen eine höhere Priorität als Zulassungsregeln. Auf diese Weise können Sie den Zugriff auf einen ganzen Bereich von Ressourcen erlauben, gleichzeitig aber auch den Zugriff auf ausgewählte Ressourcen innerhalb dieses Bereichs verweigern. Stellen Sie sich z. B. vor, Sie möchten einer Gruppe den Zugriff auf eine Ressourcengruppe im Bereich 10.20.10.0/24 erlauben, müssen dabei aber der Gruppe den Zugriff auf 10.20.10.30 verweigern. Um dies umzusetzen, müssen Sie zwei Ressourcengruppen erstellen: eine, die das Subnetz 10.20.10.0/24 enthält, und eine andere, die 10.20.10.30 enthält. Der Zugriff auf diese Ressource wird so lange verweigert, bis Sie ihn explizit erlauben.

So konfigurieren Sie die Ressourcenzugriffssteuerung für eine Gruppe:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Konfigurieren Sie im rechten Bereich die Gruppenressourcen.

   Wenn die Ressource konfiguriert ist, klicken Sie auf die Ressource und ziehen Sie sie auf die Gruppe im linken Bereich.
3. Wenn Sie den Zugriff auf eine Ressource zulassen oder verweigern möchten, klicken Sie mit der rechten Maustaste im linken Bereich auf die Netzwerkressource oder die Anwendungsrichtlinie und klicken Sie dann auf **Allow** oder **Deny**.

So entfernen Sie eine Ressource von einer Benutzergruppe:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Erweitern Sie im linken Bereich die Gruppe und dann den entsprechenden Richtlinien-Knoten.
3. Klicken Sie mit der rechten Maustaste auf die Ressource, die Sie entfernen möchten, und klicken Sie dann auf **Remove**.

Festlegen von Anwendungsrichtlinien

Anwendungsrichtlinien dienen dazu, den Netzwerkpfad einzuschränken, auf den Anwendungen zugreifen können. Stellen Sie sich z. B. vor, ein Benutzer verwendet für den E-Mail-Verkehr im Unternehmen Microsoft Outlook 2003. Sie können Outlook so konfigurieren, dass sie einen bestimmten Netzwerkpfad zum Microsoft Exchange-Server verwendet. Wenn die Netzwerkressource definiert ist, sucht Outlook beim Starten nach der Netzwerkressource und der Endpunktrichtlinie (sofern definiert). Ist die Prüfung erfolgreich, kann sich der Benutzer anmelden und seine E-Mails abrufen. Fällt die Prüfung negativ aus, startet Outlook nicht.

Wenn die Anwendung bereits vor dem Herstellen der Verbindung zum Access Gateway geöffnet ist, bleibt sie geöffnet, aber die Richtlinien werden wirksam, sodass der Benutzer die Anwendung u. U. verwenden kann.

Wenn für eine Anwendung keine Netzwerkressource oder Endpunktrichtlinie konfiguriert ist und wenn auf der Registerkarte **General** das Kontrollkästchen **Deny applications without policies** aktiviert ist, wird der Anwendung der Zugriff auf das Netzwerk verweigert.

So konfigurieren Sie eine Anwendungsrichtlinie:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **Application Policies** und klicken Sie dann auf **New Application Policy**.
3. Geben Sie einen Namen für die Ressource ein und klicken Sie auf **OK**.
4. Geben Sie unter **Application** den Namen der Anwendung ein oder klicken Sie auf **Browse**, um zur Anwendung zu navigieren und sie auszuwählen.

   Im Feld **MD5** wird automatisch die Binärsumme der Anwendung eingetragen.
5. Wenn Sie die Anwendung auf bestimmte Netzwerke beschränken möchten oder eine Endpunktrichtlinie vorhanden sein muss, führen Sie unter **Application Policies** einen der folgenden Schritte aus:
   - Wenn Sie der Anwendungsrichtlinie eine Netzwerkressource hinzufügen möchten, klicken Sie unter **Network Resources** auf die Ressource und ziehen Sie sie auf **Application network policies**.
   - Wenn Sie der Anwendungsrichtlinie eine Endpunktrichtlinie hinzufügen möchten, klicken Sie unter **End Point Policies** auf die Richtlinie und ziehen Sie sie auf **Application end point policies**.
6. Klicken Sie auf **OK**.

Durch Anwendungsrichtlinien wird der Netzwerkzugriff weiter eingeschränkt, indem einzelne Netzwerkressourcen bestimmten Anwendungen zugewiesen werden. Anwendungsrichtlinien definieren den Netzwerkpfad und die Endpunktrichtlinien für eine bestimmte Anwendung.

So fügen Sie einer Gruppe eine Anwendungsrichtlinie hinzu:

1. Klicken Sie auf der Registerkarte **Access Policy Manager** im rechten Bereich unter **Application Policies** auf die Richtlinie, die Sie hinzufügen möchten, und ziehen Sie sie dann auf die Benutzergruppe im linken Bereich.
2. Klicken Sie zum Zulassen oder Verweigern des Zugriffs mit der rechten Maustaste auf die Anwendungsrichtlinie und klicken Sie dann auf **Allow** oder **Deny**.

Wenn eine Anwendungsrichtlinie erstellt und dann einer Benutzergruppe hinzugefügt wird, kann die Anwendung nur den festgelegten Netzwerkpfad und die angegebene Endpunktrichtlinie verwenden. Andere Anwendungen werden dadurch aber nicht an der Verwendung dieser Ressourcen gehindert. Wenn Anwendungen an der Verwendung dieser Netzwerkressourcen gehindert werden sollen, können Sie den Zugriff auf das Netzwerk verweigern.

So verweigern Sie den Netzwerkzugriff für Anwendungen ohne Richtlinien:

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** auf eine Benutzergruppe und klicken Sie dann auf **Properties**.
2. Aktivieren Sie auf der Registerkarte **General** unter **Application options** die Option **Deny applications without policies**.

Es ist möglich, einer Anwendung den Zugriff auf das Netzwerk zu verweigern, während alle anderen Anwendungen auf das Netzwerk zugreifen können.

So verweigern Sie einer Anwendung den Zugriff auf das Netzwerk:

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** auf eine Benutzergruppe und klicken Sie dann auf **Properties**.
2. Deaktivieren Sie auf der Registerkarte **General** unter **Application Options** die Option **Deny applications without policies**.
3. Klicken Sie auf **OK** und schließen Sie das Dialogfeld **Properties**.
4. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **Application Policies** und klicken Sie dann auf **New Application Policy**.
5. Geben Sie einen Namen für die Richtlinie ein und klicken Sie auf **OK**.
6. Geben Sie im Bereich **Application resource** unter **Application** den Anwendungsnamen ein oder klicken Sie auf **Browse**, um die Anwendung

zu suchen und auszuwählen. Wenn dieses Feld ausgefüllt ist, wird das Feld **MD5** automatisch ausgefüllt.

7. Wenn Sie die Anwendung auf einen bestimmten Netzwerkpfad beschränken möchten, klicken Sie unter **Network Resources** auf eine Netzwerkressource und ziehen Sie sie dann auf **Application network policies**.

   Andere konfigurierte Netzwerkressourcen müssen bereits einer Benutzergruppe angehören und für sie muss die Option **Deny** festgelegt sein. Klicken Sie dazu im linken Bereich unter **Network Policies** in der Gruppe mit der rechten Maustaste auf die entsprechende Netzwerkressource und klicken Sie dann auf **Deny**. Klicken Sie auf **OK**.

8. Klicken Sie auf die Anwendungsrichtlinie und ziehen Sie sie auf die Benutzergruppe, für die sie gilt.

Benutzer können Zugriff auf alle internen Netzwerke erhalten, die zugewiesen wurden. Der Anwendung wird der Zugriff auf das Netzwerk jedoch verweigert.

Sie können auch den Zugriff aller Anwendungen auf das Netzwerk verweigern, dabei aber den Zugriff auf einen bestimmten Netzwerkpfad zulassen, um so für einen eingeschränkten Zugriff zu sorgen. Die Vorgehensweise dazu ist mit der unter „So verweigern Sie einer Anwendung den Zugriff auf das Netzwerk:“ auf Seite 130 beschriebenen Vorgehensweise identisch. Der einzige Unterschied besteht dabei, dass die Option **Deny applications without policies** nicht zu deaktivieren, sondern zu aktivieren ist. Bei Aktivierung dieser Option wird der gesamte Anwendungszugriff auf das Unternehmensnetzwerk verweigert. Wenn Sie einen Anwendungsnetzwerkzugriff zulassen möchten, konfigurieren Sie die Anwendungsrichtlinie so, dass die Anwendung akzeptiert wird. Führen Sie dazu die in der vorherigen Schrittanweisung genannten Schritte aus.

Die Benutzer erhalten nur mit der Anwendung, die explizit zugelassen wurde, Zugriff auf die interne Site. Allen anderen Anwendungen auf dem Clientcomputer ist es nicht erlaubt, auf das interne Netzwerk zuzugreifen.

Konfigurieren von Endpunktrichtlinien und -ressourcen

In diesem Abschnitt wird das Konfigurieren von Endpunktressourcen und das anschließende Erstellen einer Endpunktrichtlinie beschrieben.

Konfigurieren von Endpunktressourcen

Endpunktressourcen bieten ein zusätzliches Maß an Sicherheit, weil sie helfen sicherzustellen, dass Benutzer Verbindungen zum Access Gateway nur von Computern aus herstellen, die bestimmte Kriterien erfüllen. So können Sie z. B. festlegen, dass ein Computer bestimmte Registrierungseinträge, Dateien und/oder aktive Prozesse haben muss.

Jede Endpunktregel legt dabei fest, dass ein Computer über eines, mehrere oder alle der folgenden Merkmale verfügen muss:

- Einen Registrierungseintrag, der dem von Ihnen festgelegten Pfad, Eintragstyp und Wert entspricht.
- Eine Datei, die dem von Ihnen festgelegten Pfad, Dateinamen und Datum entspricht. Für die Datei kann auch eine Prüfsumme angegeben werden.
- Ein von Ihnen festgelegter laufender Prozess. Für den Prozess kann auch eine Prüfsumme angegeben werden.

Endpunktrichtlinien werden auf die einzelnen Gruppen angewendet, indem ein boolescher Ausdruck festgelegt wird, in dem die Endpunkt-Ressourcennamen verwendet werden. Weitere Informationen hierzu finden Sie unter „Erstellen einer Endpunktrichtlinie für eine Gruppe“ auf Seite 133.

So erstellen Sie eine Endpunktressource:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **End Point Resources** und klicken Sie dann auf **New End Point Resource**.
3. Geben Sie einen Namen ein und klicken Sie dann auf **OK**.
4. Wählen Sie unter **End point scan type** den gewünschten Regeltyp aus.

So erstellen Sie eine Prozessregel:

1. Klicken Sie auf **Process rule**.
2. Geben Sie unter **Process Name** den Namen des Prozesses ein oder klicken Sie auf **Browse**, um zu dem Prozess zu navigieren.

   Wenn ein Prozessname eingegeben ist, wird das Feld **MD5** automatisch ausgefüllt. Klicken Sie auf **OK**.

Hinweis: Informationen zum Hinzufügen einer Endpunktrichtlinie zu einer Benutzergruppe finden Sie unter „Erstellen einer Endpunktrichtlinie für eine Gruppe“ auf Seite 133.

So erstellen Sie eine Dateiregel:

1. Klicken Sie auf **File rule**.
2. Geben Sie unter **File name** den Pfad und den Dateinamen ein oder klicken Sie auf **Browse**, um zu der Datei zu navigieren.
3. Wenn ein Dateiname eingegeben ist, wird das Feld **MD5** automatisch ausgefüllt.
4. Geben Sie unter **Date** das Datum ein. Verwenden Sie dazu das folgende Format: MM/TT/JJJJ. Dies ist das Datum, an dem die Datei erstellt wurde. Klicken Sie auf **OK**.

So erstellen Sie eine Registrierungsregel:

1. Klicken Sie auf **Registry rule**.
2. Geben Sie unter **Registry path** den Pfad ein und wählen Sie einen Schlüsseltyp aus.
3. Geben Sie unter **Registry entry** den Schlüsselnamen ein.
4. Geben Sie unter **Registry value** den Wert ein, auf den der Schlüssel gesetzt werden muss, und klicken Sie auf**OK**.

So löschen Sie eine Endpunktressource:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf die Endpunktressource, die entfernt werden soll, und klicken Sie dann auf **Remove**.

Erstellen einer Endpunktrichtlinie für eine Gruppe

Sie können einen booleschen Ausdruck erstellen, indem Sie Endpunktressourcen auf den End Point Policy Expression Generator ziehen und dort ablegen. Der Generator erstellt den Ausdruck automatisch, wenn Sie die Ressourcen per Drag & Drop in den Generator ziehen. Ausdrücke können jederzeit bearbeitet werden.

Geben Sie zum Konfigurieren einer Endpunktrichtlinie für eine Gruppe einen Ausdruck an, der die Endpunktressourcen enthält, die auf die Gruppe angewendet werden sollen.

Stellen Sie sich vor, Sie erstellen die folgenden Endpunktrichtlinien:

UntRessRegEintrag

AntiVirusProzess1

AntiVirusProzess2

Ihr Endpunktrichtlinienausdruck könnte festlegen, dass eine Registrierungsprüfsumme verifizieren muss, dass die Ressource, die versucht, eine Verbindung herzustellen, zum Unternehmen gehört und dass auf der Ressource einer der Antivirusprozesse ausgeführt werden muss. Ein solcher boolescher Ausdruck würde wie folgt aussehen:

```
(UntRessRegEintrag & (AntiVirusProzess1 | AntiVirusProzess2))
```

Gültige Operatoren für Endpunktrichtlinienausdrücke:

( )	- dient zum Verschachteln von Ausdrücken, um deren Auswertung zu steuern
&	- logisches UND
|	- logisches ODER
!	- logisches NICHT

Bei Benutzern ohne Administratorrechte schlagen die Endpunktrichtlinien fehl, wenn die Richtlinie eine Datei in einer eingeschränkten Zone (z. B. C:\Dokumente und Einstellungen\Administrator) oder einen eingeschränkten Registrierungsschlüssel enthält.

Wenn ein Benutzer mehreren Gruppen angehört, besteht die für den Benutzer geltende Endpunktrichtlinie aus der Kombination der Ausdrücke für die einzelnen Gruppen des Benutzers.

So konfigurieren Sie eine Endpunktrichtlinie für eine Gruppe:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **End Point Policies** und klicken Sie dann auf **New End Point Policy**.
3. Geben Sie einen Namen ein und klicken Sie auf **OK**.

Erstellen Sie nach der Erstellung der Richtlinie den Ausdruck, indem Sie die Endpunktressourcen per Drag & Drop auf den Expression Builder ziehen.

So konstruieren Sie einen Endpunktrichtlinienausdruck:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf eine Endpunktrichtlinie und klicken Sie auf **Properties**.

   Die Eigenschaftenseite wird geöffnet und der Ressourcenbereich wird nach links verschoben.
3. Klicken Sie unter **End point policy expression** auf **Automatically build expression**.

4. Ziehen Sie eine Ressource in den Bereich **Build an end point policy** (im oberen Bereich des Dialogfelds) und legen Sie sie auf **Add end point resources**.
5. Der Ausdruck wird unter Verwendung des Identifiers **AND** erstellt. Wenn Sie den Identifier ändern möchten, klicken Sie mit der rechten Maustaste auf eine der Ressourcen und wählen Sie im Menü einen neuen Identifier aus. Klicken Sie auf **OK**.

Der Endpunktrichtlinienausdruck wird automatisch konfiguriert. Wenn Sie den Ausdruck manuell bearbeiten möchten, klicken Sie auf die Option **Automatically build expression**, um sie zu deaktivieren. Citrix empfiehlt jedoch, die Option aktiviert zu lassen, um Fehler im Ausdruck zu vermeiden.

Festlegen der Priorität von Gruppen

Bei Benutzern, die mehreren Gruppen angehören, können Sie über die Gruppenpriorität bestimmen, welche Richtlinien für den Benutzer gelten sollen. Nehmen wir z. B. einmal an, dass einige Benutzer sowohl zur Gruppe „Vertrieb“ als auch zur Gruppe „Support“ gehören. Wenn die Gruppe „Vertrieb“ in der Liste **User Groups** vor der Gruppe „Support“ steht, gelten für die Benutzer, die beiden Gruppen angehören, die Richtlinien der Gruppe „Vertrieb“. Steht die Gruppe „Support“ in der Liste vor der Gruppe „Vertrieb“, werden die Richtlinien der Gruppe „Support“ wirksam.

Die Gruppenpriorität wirkt sich auf die folgenden Richtlinien aus:

- Portalseitenkonfiguration: Hiermit wird festgelegt, welche Portalseite Benutzer beim Herstellen einer Verbindung sehen. Die Portalseite kann die Vorlage sein, die im Access Gateway enthalten ist, oder sie kann auf das Webinterface verweisen.
- Benutzertimeouts: Hiermit wird festgelegt, wie lange eine Sitzung aktiv sein kann. Es gibt folgende Timeouts:
    - Sitzungstimeouts, bei denen eine Verbindung nach einer festgelegten Zeitspanne geschlossen wird.
    - Netzwerkaktivitätstimeouts, wobei der Secure Access Client während eines festgelegten Zeitraums keinen Netzwerkverkehr feststellt.
    - Timeout bei inaktiven Sitzungen, wobei der Secure Access Client während eines festgelegten Zeitraums keine Maus- oder Tastaturaktivität feststellt.

- Aktivieren von Split DNS: Hiermit Failover auf das lokale DNS des Benutzers ermöglicht.
- Zwingen der Benutzer, sich nach einem Netzwerkausfall oder wenn der Computer aus dem Ruhezustand oder dem Standby-Modus aktiviert wird, erneut anzumelden.

Das Access Gateway berücksichtigt alle Benutzergruppen. Wenn ein Benutzer Mitglied mehrerer Gruppen ist, wenn das Kontrollkästchen **Deny applications without policies** aktiviert ist oder wenn das Kontrollkästchen **Disable desktop sharing** in einer Gruppe aktiviert ist, wird der Zugriff auf die Anwendungen des Benutzers verweigert und die Desktopfreigabe wird deaktiviert. Dies ist unabhängig von den Einstellungen in den anderen Gruppen.

Die folgenden zwei Einstellungen werden *zusammengefasst*. Diese Einstellungen werden für alle Gruppen zusammengefasst, von denen der Benutzer Mitglied ist. Die zusammengefassten Einstellungen werden dann gesammelt auf den Benutzer angewandt. Beispiel: Ein Benutzer ist Mitglied der Vertriebs- und der Supportgruppe. Wenn die Vertriebsgruppe notepad.exe und calc.exe und die Supportgruppe Internet Explorer als Endpunktrichtlinie definiert haben, werden alle diese Richtlinien auf den Benutzer angewandt.

- Kioskmoduskonfiguration: Umfasst dauerhaften Modus, die Anwendungen, die der Benutzer verwenden kann, und die Standardwebadresse, mit der der Benutzer eine Verbindung herstellt.
- Endpunktrichtlinien: Hiermit werden Registrierungseinstellungen, Prozesse oder Dateien festgelegt, die auf dem Clientcomputer vorhanden sein müssen.

Wenn Benutzer Mitglied in mehreren Gruppen sind und IP-Pooling in einer dieser Gruppen aktiviert ist, teilt das Access Gateway der ersten Gruppe, in der IP-Pooling aktiviert ist, eine IP-Adresse aus dem Pool zu.

Gruppen werden zunächst in der Reihenfolge ihrer Erstellung aufgeführt.

So legen Sie die Priorität von Gruppen fest:

1. Klicken Sie auf die Registerkarte **Group Priority**.
2. Wählen Sie eine Gruppe aus, die verschoben werden soll, und verschieben Sie die Gruppe mit den Pfeilschaltflächen in der Liste nach oben oder unten.

   Die Gruppe, die in der Liste ganz oben steht, hat die höchste Priorität.

So zeigen Sie die Gruppenprioritäten für einen Benutzer an:

Klicken Sie im Administration Desktop auf das Symbol für den Citrix Real-time Monitor.

Es werden alle Gruppen, zu denen der Benutzer gehört, und die Gruppe mit der höchsten Priorität angezeigt.

Konfigurieren von Richtlinien zur Überprüfung vor der Authentifizierung

Mit Vorauthentifizierungsrichtlinien können Benutzer von der Anmeldung am Access Gateway ausgeschlossen werden. Wenn Benutzer zum Herstellen einer Verbindung zum Access Gateway einen Webbrowser verwenden, prüft die Vorauthentifizierungsrichtlinie den Clientcomputer, bevor das Anmeldedialogfeld angezeigt wird. Wenn die Prüfung ein negatives Ergebnis ausgibt, können sich die Benutzer nicht anmelden. Zum Anmelden am Webportal muss der Client die richtigen Anwendungen installieren.

So erstellen Sie Richtlinien zur Überprüfung vor der Authentifizierung:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Wählen Sie unter **End Point Policies** die konfigurierte Richtlinie aus und ziehen Sie sie in den linken Bereich auf **Pre-Authentication Policies** (unter dem Richtlinienknoten **Global Policies**).

Informationen zum Erstellen und Konfigurieren von Endpunktressourcen und -richtlinien finden Sie unter „Konfigurieren von Endpunktrichtlinien und -ressourcen“ auf Seite 131.

Konfigurieren von Benutzerverbindungen für den Secure Access Client

In diesem Kapitel werden Benutzerverbindungen erläutert sowie die Verfahren, mit denen Benutzer über den Secure Access Client eine Verbindung zum Access Gateway und den Unternehmensressourcen herstellen.

Benutzerverbindungen werden mit sicheren Verbindungen wie folgt aufgebaut:

- Über einen Webbrowser, der eine Verbindung zum Access Gateway herstellt
- Über die ausführbare Datei des Secure Access Clients, die auf dem Clientcomputer installiert ist

Bei der Verbindungsherstellung wird ein sicherer Tunnel zum Unternehmensnetzwerk gebildet und das Access Gateway übernimmt den SSL-Handshake. In diesem Kapitel werden die folgenden Themen behandelt:

- Systemvoraussetzungen
- Unterstützung für den Secure Access Client
- Konfigurieren von Proxyservern für den Secure Access Client
- Herstellen einer Verbindung mit einer Webadresse
- Verbindungen im Kioskmodus
- Konfigurieren der Authentizierungsanforderungen nach einer Netzwerkunterbrechung
- Konfigurieren weiterer Gruppeneigenschaften
- Schließen und Deaktivieren von Benutzerverbindungen
- Anfordern von Clientzertifikaten für die Authentifizierung
- Installieren von Stammzertifikaten
- Auswählen einer Verschlüsselungsart für Clientverbindungen

Systemvoraussetzungen

Der Secure Access Client wird von folgenden Betriebssystemen und Webbrowsern unterstützt.

Betriebssysteme

Der Secure Access Client wird von folgenden Windows-Betriebssystemen unterstützt:

- Windows XP Home Edition
- Windows XP Professional
- Windows 2000 Server
- Windows Server 2003

Der Secure Access Client wird von folgenden Linux-Betriebssystemen unterstützt:

- Red Hat Enterprise Linux 4
- SUSE Linux 10.0
- Fedora Core 4

Webbrowser

Der Secure Access Client wird von folgenden Webbrowsern unterstützt:

- Microsoft Internet Explorer, Versionen 6.*x* und 7.*x*
- Mozilla Firefox Version 1.5
- Apple Safari Versionen 1.2 und 2

Wenn Clients die Verbindung über Mozilla Firefox herstellen, können Seiten, für die ActiveX erforderlich ist (z. B. die Seite mit der Überprüfung vor der eigentlichen Authentifizierung), nicht ausgeführt werden.

Wenn Clients die Verbindung über den Kiosk herstellen, muss Sun Java Runtime Environment (JRE) Version 1.5.0_06 auf dem Computer installiert sein.

Funktionsweise von Benutzerverbindungen

Das Access Gateway funktioniert folgendermaßen:

- Wenn ein Benutzer zum ersten Mal eine Verbindung über eine Webadresse herstellt, wird der Secure Access Client heruntergeladen und auf dem Clientcomputer installiert.
- Nach dem Herunterladen des Secure Access Clients meldet sich der Benutzer an. Wenn die Authentifizierung des Benutzers erfolgreich war, richtet das Access Gateway einen sicheren Tunnel ein.
- Sobald der Remotebenutzer versucht, über den VPN-Tunnel auf die Netzwerkressourcen zuzugreifen, verschlüsselt der Secure Access Client den gesamten Netzwerkverkehr, der für das Intranet der Organisation bestimmt ist, und leitet die Pakete an das Access Gateway weiter.
- Das Access Gateway fungiert als Endpunkt des SSL-Tunnels (terminiert den Tunnel), akzeptiert den eingehenden Verkehr, der für das private Netzwerk bestimmt ist, und leitet den Verkehr an das private Netzwerk weiter. Das Access Gateway sendet den Verkehr über einen sicheren Tunnel zum Remotecomputer zurück.

Wenn ein Remotebenutzer sich über den Secure Access Client anmeldet, fordert das Access Gateway den Benutzer auf, sich über HTTP 401 Basic oder Digest zu authentifizieren. Das Access Gateway authentifiziert die Anmeldeinformationen mit einem Authentifizierungsverfahren, z. B. mit der lokalen Authentifizierung, RSA SecurID, SafeWord, LDAP, NTLM oder RADIUS. Wenn die Anmeldeinformationen korrekt sind, schließt das Access Gateway den Handshake mit dem Client ab. Dieser Anmeldeschritt ist nur dann erforderlich, wenn ein Benutzer den Secure Access Client zum ersten Mal herunterlädt.

Wenn sich der Benutzer hinter einem Proxyserver befindet, kann er den Proxyserver und die Authentifizierungsinformationen angeben. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Proxyservern für den Secure Access Client“ auf Seite 148.

Der Secure Access Client wird auf dem Computer des Benutzers installiert. Nachdem die erste Verbindung hergestellt wurde, kann der Benutzer beim nächsten Mal die Desktopverknüpfung verwenden, um den Secure Access Client zu starten.

Im Dialogfeld **Erweiterte Optionen** werden die Einstellungen für den Clientcomputer konfiguriert. Zum Öffnen dieses Dialogfelds können Sie auch mit der rechten Maustaste auf das Citrix Secure Access Client-Symbol auf dem Desktop klicken und im Kontextmenü die Option **Eigenschaften** wählen.

Einrichten des sicheren Tunnels

Nachdem der Secure Access Client gestartet wurde, richtet er einen sicheren Tunnel über den Port 443 (oder jeden anderen konfigurierten Port des Access Gateways) ein und sendet Authentifizierungsinformationen. Nachdem der Tunnel eingerichtet wurde, sendet das Access Gateway Konfigurationsinformationen an den Secure Access Client, in denen beschrieben wird, welche Netzwerke gesichert werden sollen. Außerdem enthalten diese Informationen eine IP-Adresse, sofern IP-Pooling aktiviert wurde. Weitere Informationen über IP-Pooling finden Sie unter „Aktivieren von IP-Pooling“ auf Seite 168.

Tunneln des privaten Netzwerkverkehrs über sichere Verbindungen

Sobald der Secure Access Client gestartet und der Benutzer authentifiziert wurde, wird der gesamte Netzwerkverkehr, der für die angegebenen privaten Netzwerke bestimmt ist, über den sicheren Tunnel an das Access Gateway weitergeleitet.

Das Access Gateway fängt alle vom Clientgerät hergestellten Netzwerkverbindungen ab und multiplext/tunnelt diese über SSL an das Access Gateway, wo der Verkehr demultiplext wird und die Verbindungen an die korrekte Kombination aus Host und Port weitergeleitet werden.

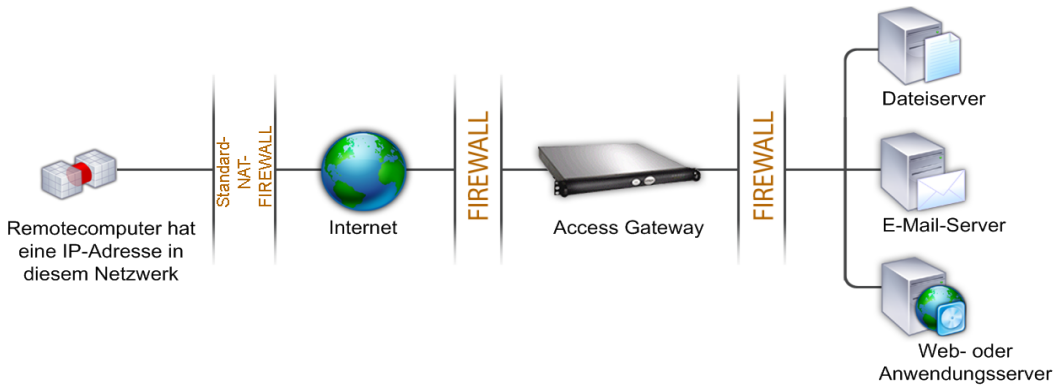
Die Verbindungen unterliegen administrativen Sicherheitsrichtlinien für einzelne Anwendungen, einen Teilsatz von Anwendungen oder das gesamte Intranet. Sie legen die Ressourcen fest (Paare aus IP-Adressbereichen/Subnetzmasken), auf die die Remotebenutzer über die VPN-Verbindung zugreifen können. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Netzwerkzugriff und Gruppenressourcen“ auf Seite 113.

Alle IP-Pakete, gleich welchen Protokolls, werden abgefangen und über eine sichere Verbindung weitergeleitet. Von lokalen Anwendungen auf dem Clientcomputer ausgehender Verkehr wird sicher durch den Tunnel zum Access Gateway geleitet, der dann die Verbindungen mit dem Zielserver wiederherstellt. Für die Zielserver sehen die Verbindungen so aus, als stammten sie vom lokalen Access Gateway im privaten Netzwerk, sodass die IP-Adresse des Clients verborgen wird. Dieses Verfahren wird auch *Reverse NAT* (Network Address Translation) genannt. Das Verbergen der IP-Adressen erhöht die Sicherheit der Standorte, von denen der Verkehr ausgeht.

Lokal, also auf dem Clientcomputer, wird der gesamte verbindungsspezifische Verkehr (wie SYN-ACK-, PUSH-, ACK- und FIN-Pakete) vom Secure Access Client neu erstellt, damit es so aussieht, als käme er vom privaten Server.

Funktionsweise bei Verwendung von Firewalls und Proxyservern

Unter Umständen befinden sich Benutzer des Secure Access Clients innerhalb der Firewall einer anderen Organisation, wie in der folgenden Abbildung dargestellt.



Remoteclientverbindung durch zwei Unternehmensfirewalls

NAT-Firewalls verfügen über eine Tabelle, mit deren Hilfe sie sichere Pakete vom Access Gateway zum Clientcomputer zurücksenden können. Für schaltungsorientierte Verbindungen unterhält das Access Gateway eine portzugeordnete Reverse-NAT-Übersetzungstabelle. Die Reverse-NAT-Übersetzungstabelle versetzt das Access Gateway in die Lage, Verbindungen zuzuordnen und Pakete mit den richtigen Portnummern über den Tunnel zurück an den Client zu senden, sodass die Pakete zur korrekten Anwendung zurückkehren.

Bei der Herstellung des Access Gateway-Tunnels kommen als Industriestandard anerkannte Verbindungsherstellungsmethoden wie HTTPS, Proxy HTTPS und SOCKS zum Einsatz. Auf diese Weise wird sichergestellt, dass die Access Gateway-Firewall zugänglich ist und den Remotecomputern die Möglichkeit gibt, von ihrem Standort innerhalb der Firewalls anderer Unternehmen aus auf private Netzwerke zuzugreifen, ohne dass es dabei zu Problemen kommt.

So kann die Verbindung beispielsweise über einen Zwischenproxy, wie einen HTTP-Proxy, hergestellt werden, indem ein CONNECT HTTPS-Befehl an den Zwischenproxy gesendet wird. Alle Anmeldeinformationen, die der Zwischenproxy benötigt, werden wiederum vom Remotebenutzer bezogen (über die Single Sign-On-Informationen oder eine Aufforderung zur Eingabe der entsprechenden Informationen) und dann dem Zwischenproxyserver bereitgestellt. Nachdem die HTTPS-Sitzung eingerichtet wurde, wird der eigentliche Datenverkehr verschlüsselt und in Form von sicheren Paketen an das Access Gateway gesendet.

Beenden des sicheren Tunnels und Zurücksenden von Paketen an den Client

Das Access Gateway beendet den SSL-Tunnel und akzeptiert eingehende Pakete, die für das private Netzwerk bestimmt sind. Wenn die Pakete die Autorisierungs- und Zugriffssteuerungskriterien erfüllen, erzeugt das Access Gateway die IP-Header der Pakete neu, sodass sie aussehen, als stammten sie aus dem IP-Adressbereich des privaten Netzwerks, in dem sich das Access Gateway befindet, oder von der vom Client zugewiesenen privaten IP-Adresse. Das Access Gateway sendet die Pakete dann an das Netzwerk.

Hinweis: Der Secure Access Client unterhält zwei Tunnel: einen SSL-Tunnel, über den Daten an das Access Gateway gesendet werden, und einen Tunnel zwischen dem Client und den lokalen Anwendungen. Die verschlüsselten Daten, die über den SSL-Tunnel ankommen, werden dann entschlüsselt, bevor sie über den zweiten Tunnel an die lokale Anwendung gesendet werden.

Wenn auf dem Computer, auf dem der Secure Access Client ausgeführt wird, ein Paketsniffer in Betrieb ist (z. B. Ethereal), wird unverschlüsselter Verkehr angezeigt, der scheinbar zwischen dem Client und dem Access Gateway ausgetauscht wird. Dieser unverschlüsselte Verkehr läuft jedoch nicht über den Tunnel zwischen dem Client und dem Access Gateway, sondern über den Tunnel zu den lokalen Anwendungen.

Wenn ein Anwendungsclient eine Verbindung mit seinem Anwendungsserver herstellt, kann es vorkommen, dass bestimmte Protokolle verlangen, dass der Anwendungsserver im Gegenzug versucht, eine neue Verbindung mit dem Client herzustellen. In diesem Fall sendet der Client mittels eines individuellen Client-Server-Protokolls seine bekannte lokale IP-Adresse an den Server. Für diese Anwendungen stellt der Secure Access Client der lokalen Clientanwendung die Repräsentation einer privaten IP-Adresse zur Verfügung, die das Access Gateway im internen Netzwerk verwendet. Dieses Feature wird von vielen Echtzeit-Sprachanwendungen und von FTP verwendet.

Clients können auf die Ressourcen im Unternehmensnetzwerk zugreifen, indem sie über das Access Gateway eine Verbindung von ihrem eigenen Computer oder von einem öffentlichen Computer aus herstellen. Die Funktionsweise von Clientverbindungen wird in den folgenden Themen genauer beschrieben:

- Unterstützung für den Secure Access Client
- Konfigurieren von Proxyservern für den Secure Access Client
- Herstellen einer Verbindung mit einer Webadresse
- Verbindungen im Kioskmodus
- Konfigurieren der Authentizierungsanforderungen nach einer Netzwerkunterbrechung
- Konfigurieren weiterer Gruppeneigenschaften
- Schließen und Deaktivieren von Benutzerverbindungen
- Anfordern von Clientzertifikaten für die Authentifizierung
- Installieren von Stammzertifikaten
- Auswählen einer Verschlüsselungsart für Clientverbindungen
- Unterstützung von VoIP-Softphones

Unterstützung für den Secure Access Client

Damit die Benutzer eine Verbindung zum Access Gateway herstellen und es verwenden können, müssen Sie die folgenden Informationen bereitstellen:

- Webadresse für das Access Gateway (z. B. https://*AccessGatewayFQDN*/).

  Wenn ein Benutzer von einem Computer aus zugreifen muss, auf dem weder Windows 2000 oder höher noch Linux ausgeführt wird, jedoch Java Virtual Machine (JVM) 1.5 oder höher vorliegt, kann der Benutzer die Java-Appletversion des Kiosks verwenden. Die Webadresse für das Herstellen einer Verbindung zur Java-Appletversion des Kiosks lautet:

  https://*AccessGateway*/vpn_portal-javaonly.html

- Für die Anmeldung erforderlicher Name des Authentifizierungsbereichs (sofern Sie nicht den Bereich **Default** verwenden).
- Pfad zu allen Netzlaufwerken, auf die die Benutzer zugreifen können sollen; erfolgt durch Zuordnen eines Netzlaufwerks auf deren Computer.
- Sämtliche Systemvoraussetzungen für das Ausführen des Secure Access Clients, sofern Endpunktressourcen und -richtlinien konfiguriert wurden.

Abhängig von der Konfiguration des Systems des Remotebenutzers müssen Sie darüber hinaus u. U. noch weitere Informationen bereitstellen:

- Um den Secure Access Client starten zu können**,** müssen Windows 2000-Benutzer als lokaler Administrator oder als Mitglied der Administratorgruppe angemeldet sein, damit sie berechtigt sind, Programme auf dem Computer zu installieren. Bei Windows XP gilt diese Einschränkung nur für die Erstinstallation – Aktualisierungen und Upgrades können auch ohne Administratorrechte installiert werden.
- Wenn auf dem Remotecomputer eine Firewall installiert und aktiviert ist, muss der Benutzer u. U. die Firewalleinstellungen so ändern, dass der Verkehr zu oder von den IP-Adressen der Ressourcen, auf die er zugreifen darf, nicht blockiert wird. Die Internetverbindungsfirewall von Windows XP und die Windows-Firewall von Windows XP Service Pack 2 werden vom Secure Access Client automatisch angepasst. Weitere Informationen zum Konfigurieren verschiedener gängiger Firewalls finden Sie unter „Konfigurieren persönlicher Firewalls von Drittanbietern“ auf Seite 267.
- Benutzer, die die Access Gateway-Verbindung für FTP verwenden möchten, müssen ihre FTP-Anwendung so einrichten, dass sie passive Übertragungen unterstützt. Eine passive Übertragung bedeutet, dass der Remotecomputer die Datenverbindung zu Ihrem FTP-Server und nicht Ihr FTP-Server die Datenverbindung zum Remotecomputer einrichtet.
- Benutzer, die die Verbindung für die Ausführung von X-Client-Anwendungen verwenden möchten, müssen auf ihren Computern einen X-Server ausführen, z. B. XManager.

Da die Benutzer mit den Dateien und Anwendungen arbeiten, als würden sie sich lokal im Netzwerk der Organisation befinden, ist keine Schulung der Benutzer und keine Konfiguration der Anwendungen nötig.

Für die in diesem Abschnitt besprochenen Informationen gibt es auf der Seite **Downloads** des Administration Portals eine entsprechende E-Mail-Vorlage. Citrix empfiehlt, den Text für Ihre Site anzupassen und die E-Mail dann an die Benutzer zu senden.

Konfigurieren von Proxyservern für den Secure Access Client

Wenn der Secure Access Client eine Verbindung herstellt, fragt der Secure Access Client zunächst die Clientproxyeinstellungen im Betriebssystem ab, bevor die Richtlinien vom Access Gateway heruntergeladen werden. Ist die automatische Erkennung aktiviert, stellt der Secure Access Client die Clientproxyeinstellungen automatisch auf die Einstellungen ein, die im Betriebssystem gespeichert sind. Der Secure Access Client baut eine Verbindung zum Access Gateway auf, lädt die Vorauthentifizierungsrichtlinien herunter und fordert die Benutzer dann zur Eingabe ihrer Anmeldeinformationen auf. Falls der Secure Access Client die Clientproxyeinstellungen nicht automatisch erkennt, wird eine direkte Verbindung ohne den Umweg über den Proxyserver hergestellt. Die automatische Erkennung der Proxyeinstellungen wird im Secure Access Client im Dialogfeld **Erweiterte Optionen** konfiguriert.

Außerdem können die Benutzer einen Proxyserver manuell über den Secure Access Client konfigurieren. Bei der manuellen Konfiguration eines Proxyservers wird die automatische Erkennung der Proxyeinstellungen deaktiviert.

So konfigurieren Sie einen Proxyserver manuell:

1. Klicken Sie auf dem Desktop des Clientcomputers auf das Symbol für den Secure Access Client. Das Anmeldedialogfeld wird geöffnet.
2. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle des **Secure Access Client**-Anmeldedialogfelds und wählen Sie **Erweiterte Optionen**.
3. Aktivieren Sie im Dialogfeld **Citrix Secure Access-Optionen** unter **Proxyeinstellungen** die Option **Proxyserver manuell konfigurieren**.
4. Geben Sie in den Feldern **IP-Adresse** und **Port** die IP-Adresse und die Portnummer ein.
5. Wenn der Server eine Authentifizierung erfordert, wählen Sie **Proxyserver erfordert Authentifizierung**.

Das Dialogfeld **Erweiterte Optionen** kann auch geöffnet werden, indem Sie mit der rechten Maustaste auf das Citrix Secure Access-Symbol auf dem Desktop klicken und im Kontextmenü die Option **Eigenschaften** wählen.

Konfigurieren des Secure Access Clients für Benutzer ohne Administratorrechte

Ist ein Benutzer auf einem Computer mit Windows 2000 Professional nicht als Administrator angemeldet, muss der Secure Access Client lokal auf dem Clientcomputer installiert und dann über die Webadresse https://*FQDN*/citrixsaclient.exe gestartet werden; *FQDN* bezeichnet hierbei die Adresse des Access Gateways. Das ActiveX-Applet ist nicht mit den nötigen Rechten ausgestattet, um die Datei herunterzuladen und zu installieren. Clients, die an Windows 2003 Server oder Windows XP als Nicht-Administratoren angemeldet sind, können das ActiveX-Applet herunterladen und installieren.

Ein Benutzer, der nicht als Administrator angemeldet ist und die Verbindung über den Secure Access Client herstellt, muss damit rechnen, dass Anwendungen wie Microsoft Outlook gelegentlich die Verbindung zum Netzwerk verlieren.

Konfigurieren von Single Sign-on für Windows-Betriebssysteme

Standardmäßig öffnen Windows-Benutzer eine Verbindung, indem sie den Secure Access Client vom Desktop aus starten. Durch Aktivieren von Single Sign-On können Sie festlegen, dass der Secure Access Client automatisch gestartet wird, wenn sich der Benutzer an Windows anmeldet. Ist Single Sign-on konfiguriert, werden die Windows-Anmeldeinformationen des Benutzers zur Authentifizierung an das Access Gateway weitergegeben.

Aktivieren Sie Single Sign-On nur, wenn sich die Computer der Benutzer an der Domäne Ihrer Organisation anmelden. Wenn Single Sign-On aktiviert ist und ein Benutzer eine Verbindung von einem Computer herstellt, der sich nicht in Ihrer Domäne befindet, wird der Benutzer aufgefordert, sich anzumelden.

Hinweis: Voraussetzung für die Nutzung von Single Sign-On für den Secure Access Client unter Windows ist die Anmeldung als Hauptbenutzer oder die Mitgliedschaft in der Gruppe der Hauptbenutzer.

Wenn der Secure Access Client für den Single Sign-On-Betrieb unter Windows konfiguriert ist, wird er automatisch gestartet, sobald sich der Benutzer an Windows anmeldet. Die Windows-Anmeldeinformationen des Benutzers werden zur Authentifizierung an das Access Gateway weitergegeben. Durch das Konfigurieren der Single Sign-On-Funktionalität für den Secure Access Client wird der Remotecomputer u. a. in die Lage versetzt, Installationsskripte aus- und automatische Laufwerkszuordnungen durchzuführen.

So konfigurieren Sie den Secure Access Client für Single Sign-On unter Windows:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **General** unter **Session options** die Option **Enable single sign-on with Windows**.
4. Klicken Sie auf **OK**.

Hinweis: Wenn Sie Zweimethodenauthentifizierung konfiguriert haben, ist die Verwendung von Single Sign-On nicht möglich.

Herstellen von Verbindungen mit früheren Versionen des Secure Access Clients

Sie können das Access Gateway so konfigurieren, dass auch Verbindungen von früheren Versionen des Secure Access Clients akzeptiert werden, z. B. dass das Access Gateway 4.5 Verbindungen vom Secure Access Client 4.2 akzeptiert.

Wenn auch frühere Versionen des Secure Access Clients eine Verbindung zum Access Gateway herstellen sollen, legen Sie 3DES oder RC4 als Verschlüsselungsart für Clientverbindungen fest. Frühere Versionen des Secure Access Clients unterstützen keine AES-Verschlüsselung und können keine Verbindung aufbauen, wenn AES aktiviert ist.

So ermöglichen Sie die Verbindungsherstellung zum Access Gateway mit früheren Versionen des Secure Access Clients:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie **Allow connections using earlier versions of the Secure Access Client**.
3. Klicken Sie auf **Submit**.

Aktualisieren früherer Versionen des Secure Access Clients

Es gibt eine globale Einstellung, mit der die Aufforderung zur Aktualisierung einer früheren Version des Secure Access Clients gesteuert wird. Diese Einstellung ist für künftige Versionen des Secure Access Clients reserviert.

Wenn Sie diese Einstellung aktivieren und ein Benutzer über eine frühere Version des Secure Access Clients eine Verbindung zum Access Gateway herstellt, wird der Benutzer aufgefordert, den Client zu aktualisieren.

Bei Secure Access Client-Versionen vor 4.5 ist diese Einstellung wirkungslos. Bei diesen Versionen wird der Benutzer durch eine integrierte Funktion zur Aktualisierung aufgefordert, wenn er versucht, eine Verbindung zu einer höheren Version des Access Gateways herzustellen.

Ist diese Einstellung aktiviert, wird der Benutzer zur Aktualisierung aufgefordert, wenn die beiden folgenden Bedingungen erfüllt sind:

- Der zu Access Gateway Version 4.5 gehörige Secure Access Client wird (in der Zukunft) durch eine aktualisierte Version ersetzt.
- Ein Benutzer stellt über Secure Access Client Version 4.5 eine Verbindung zum Access Gateway her.

So lassen Sie eine Aufforderung zur Aktualisierung früherer Versionen des Secure Access Clients anzeigen:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie **Prompt to upgrade earlier versions of the Secure Access Client**.
3. Klicken Sie auf **Submit**.

Herstellen einer Verbindung mit einer Webadresse

Wenn Benutzer eine Verbindung über eine Webseite herstellen, werden sie entweder aufgefordert, sich anzumelden, oder sie werden direkt an eine Portalseite weitergeleitet, auf der sie die Verbindung über den Secure Access Client herstellen können.

Ist der Access Gateway so konfiguriert, dass die Benutzer sich anmelden müssen, bevor sie eine Verbindung über den Secure Access Client herstellen können, geben sie zur Anmeldung ihren Benutzernamen und ihr Kennwort ein. Eine Portalseite wird geöffnet, auf der Benutzer sich wahlweise über den kompletten Secure Access Client oder auch im Kioskmodus (sofern aktiviert) anmelden. Wenn ein Benutzer sich über den Secure Access Client anmeldet, bietet die Verbindung uneingeschränkten Zugriff auf die Netzwerkressourcen, auf die die Gruppen, denen der Benutzer angehört, zugreifen dürfen.

Der entsprechend den Sicherheitsrichtlinien gewährte Zugriff versetzt die Benutzer in die Lage, mit dem Remotesystem genau so zu arbeiten, als wären sie lokal angemeldet. So kann den Benutzern z. B. der Zugriff auf Webanwendungen, Client-Server- und Peer-to-Peer-Anwendungen, wie Instant-Messaging-, Videoconferencing- und Echtzeit-VoIP-Anwendungen, gewährt werden. Die Benutzer können auch Netzlaufwerke zuordnen, um auf für sie zugängliche Netzwerkressourcen, wie z. B. freigegebene Ordner und Drucker, zuzugreifen.

Während der Verbindung mit dem Access Gateway können Remotebenutzer keine Netzwerkinformationen von der Site aus sehen, mit der sie verbunden sind. Geben Sie z. B. an einer Eingabeaufforderung Folgendes ein, während Sie mit dem Access Gateway verbunden sind:

ipconfig/all or route print

Es werden keine aus dem Unternehmensnetzwerk stammenden Netzwerkinformationen angezeigt.

Installieren von ActiveX Helper

Wenn der Benutzer eine Verbindung zur Webportalseite herstellt und sich anmeldet, wird net6helper.cab (ein ActiveX-Steuerelement) installiert. Diese Datei bietet die folgenden drei Hauptfunktionen:

- Sie startet den Client von der Webseite aus – der Secure Access Client muss also nicht erst heruntergeladen und gestartet werden.
- Sie führt für die Webseite Überprüfungen vor der Authentifizierung durch.
- Sie bietet Single Sign-On-Funktionalität unter Windows für den gesamten Client. Wenn der Secure Access Client von der Webseite aus gestartet wird, wird der Benutzer nicht aufgefordert, sich erneut anzumelden.

Anmelden mit dem Secure Access Client

Wenn der Secure Access Client geladen ist, werden die Benutzer aufgefordert, sich am Access Gateway anzumelden, damit die Verbindung hergestellt wird. Der Access Gateway-Administrator legt auf der Registerkarte **Authentication** im Administration Tool den Typ der Authentifizierung fest. Weitere Informationen hierzu finden Sie unter „Konfigurieren der Authentifizierung und Autorisierung“ auf Seite 77.

Wenn auf dem Access Gateway Zweimethodenauthentifizierung konfiguriert ist und die Benutzer sich mit vollen Zugriffsberechtigungen anmelden, müssen sie für jedes Authentifizierungsverfahren den entsprechenden Benutzernamen und das zugehörige Kennwort eingeben. So könnte z. B. festgelegt werden, dass die Benutzer die LDAP-Authentifizierung und RSA SecurID verwenden müssen. In diesem Fall müssten die Benutzer ihr Kennwort, ihre RSA SecurID-PIN und den RSA SecurID-Code eingeben. Weitere Informationen zum Anmelden mit Zweimethodenauthentifizierung finden Sie unter „Anmelden mit Zweimethodenauthentifizierung“ auf Seite 191.

Hinweis: Bei Verwendung des Linux-Clients sind die in der folgenden Prozedur beschriebenen Optionen im Verbindungsfenster nicht vorhanden.

Der Secure Access Client wird installiert, sobald der Benutzer sich erstmals bei der Portalwebseite anmeldet.

So installieren Sie den Secure Access Client:

1. Geben Sie in einem Webbrowser die Webadresse des Access Gateways ein (z. B. *https://www.meinefirma.com*).
2. Falls das Access Gateway eine Anmeldung erfordert, geben Sie den Benutzernamen und das Kennwort ein und klicken Sie auf **Anmelden**.
3. Wählen Sie auf der Portalseite des Citrix Access Gateways die Option **Eigener Computer** und klicken Sie auf **Verbinden**.

   Der Benutzer wird aufgefordert, das ActiveX-Steuerelement net6helper.cab zu installieren.
4. Folgen Sie den Anweisungen auf dem Bildschirm, um den Secure Access Client zu installieren.

   Nach erfolgter Installation wird ein Symbol auf dem Desktop angezeigt.

So melden Sie sich über den Secure Access Client am Access Gateway an:

1. Doppelklicken Sie auf dem Desktop auf das Symbol des Secure Access Clients.
2. Geben Sie im Dialogfeld **Citrix Secure Access Client** die Anmeldeinformationen ein.

   Wenn das Access Gateway mit mehreren Authentifizierungsbereichen konfiguriert ist und eine Verbindung zu einem anderen Bereich als dem Bereich **Default** hergestellt werden soll, geben Sie vor dem Benutzernamen den Bereichsnamen ein (*Bereichsname**Benutzername*).

   Falls SafeWord-Produkte von Secure Computing verwendet werden, geben Sie den Passcode ein.
3. Wenn das Access Gateway die Zweimethodenauthentifizierung erfordert, geben Sie für jedes Authentifizierungsverfahren den entsprechenden Benutzernamen und das zugehörige Kennwort ein.

   Wenn Ihre Site die RSA SecurID-Authentifizierung verwendet, setzt sich Ihr Kennwort aus Ihrer PIN und der auf dem RSA SecurID-Token angezeigten Zahl zusammen.

.

Secure Access Client-Dialogfeld für die Zweimethodenauthentifizierung

4. Sollen die Einstellungen geändert werden, klicken Sie mit der rechten Maustaste auf das Dialogfeld und klicken Sie dann auf **Erweiterte Optionen**. Sie können die folgenden Einstellungen ändern:

   - **Webadresse** des Geräts: Hier werden außerdem die IP-Adressen oder vollqualifizierten Domänennamen der letzten 10 Geräte aufgeführt, zu denen der Benutzer eine Verbindung hergestellt hat.
   - **Proxyeinstellungen** für den Clientcomputer: Benutzer können automatische Proxyservererkennung festlegen oder einen Proxyserver manuell konfigurieren.
   - **Aktivieren von Split DNS:** Diese Einstellung wird im Administration Tool festgelegt. Ist diese Einstellung nicht verfügbar, sind entsprechend keine Änderungen möglich. Weitere Informationen über Split DNS finden Sie unter „Aktivieren von Split DNS“ auf Seite 169.
   - **Deaktivieren von Sicherheitszertifikatswarnungen:** Falls kein von einer Zertifizierungsstelle signiertes sicheres Zertifikat installiert ist, wird eine Zertifikatswarnung eingeblendet, sobald sich ein Benutzer anmeldet. Diese Einstellung deaktiviert die Warnung.

Kontextmenü des Secure Access Client-Dialogfelds

5. Sie können das zweite Kennwortfeld ein- und ausblenden. Führen Sie hierzu einen der folgenden Schritte aus:

   - Wird das Feld für das sekundäre Kennwort angezeigt, klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im Dialogfeld und wählen Sie im Menü die Option **Sekundäres Kennwort ausblenden**.
   - Wird das Feld für das sekundäre Kennwort nicht angezeigt, klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im Dialogfeld und wählen Sie im Menü die Option **Sekundäres Kennwort anzeigen**.

   Hinweis: Die Kennwortbeschriftungen im Dialogfeld **Secure Access Client** können im Administration Tool auf der Registerkarte **Authentication** geändert werden. Falls Sie die Kennwortbeschriftungen geändert haben, wird dieser Text im **Secure Access Client**-Dialogfeld und auf der Anmeldewebseite angezeigt. Die Menüoption zum Ein- und Ausblenden der Kennwortbeschriftungen bleibt unverändert. Weitere Informationen hierzu finden Sie unter „Ändern der Beschriftung von Kennwortfeldern“ auf Seite 111.

6. Klicken Sie auf **Verbinden**.

Hinweis: Wenn das auf dem Access Gateway installierte digitale Zertifikat nicht von einer Zertifizierungsstelle signiert ist, wird eine Sicherheitswarnung angezeigt. Weitere Informationen finden Sie unter „Erstellen und Installieren von Zertifikaten“ auf Seite 55 und „Sichern von Verbindungen mit digitalen Zertifikaten“ auf Seite 291.

Wenn die Verbindung hergestellt ist, wird kurz ein Statusfenster angezeigt und das Secure Access Client-Fenster wird auf ein Symbol im Infobereich der Taskleiste minimiert. Das Symbol zeigt an, ob die Verbindung aktiviert oder deaktiviert ist, und es blinkt, während Aktivitäten stattfinden.

So zeigen Sie die Secure Access Client-Statuseigenschaften an:

Doppelklicken Sie im Infobereich auf das Secure Access Client-Verbindungssymbol. Sie können stattdessen auch mit der rechten Maustaste auf das Symbol klicken und im Kontextmenü den Befehl **Eigenschaften** wählen.

Das Dialogfeld **Citrix Secure Access Client** wird angezeigt.

Die Verbindungseigenschaften enthalten nützliche Informationen für die Problembehandlung. Hierzu gehören z. B. folgende Eigenschaften:

- Die Registerkarte **Allgemein** enthält Verbindungsinformationen.
- Auf der Registerkarte **Details** finden Sie Serverinformationen und eine Liste der gesicherten Netzwerke, auf die der Client zugreifen kann.
- Die Registerkarte **Zugriffslisten** enthält die Zugriffssteuerungslisten (ACLs), die für die Benutzerverbindung konfiguriert sind. Diese Registerkarte wird nur für Benutzer angezeigt, die Mitglied einer Gruppe sind. Wenn für eine Gruppe keine Zugriffssteuerungsliste konfiguriert ist, wird die Registerkarte auch nicht angezeigt.

Klicken Sie zum Schließen des Fensters auf **Schließen**.

So trennen Sie die Verbindung zum Secure Access Client:

Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Secure Access-Symbol und wählen Sie im Kontextmenü den Befehl **Trennen**.

Verbindungen im Kioskmodus

Das Access Gateway bietet zur Sicherung des Verkehrs zwischen öffentlichen Computern und Unternehmensnetzwerken einen Kioskmodus. Wenn Benutzer auf der Seite **Citrix Access Portal** die Option **Öffentlicher Computer** wählen, wird ein Webbrowser geöffnet. Der Benutzer meldet sich an und kann dann auf die im Browserfenster angezeigten Anwendungen zugreifen.

Standardmäßig ist der Kioskmodus deaktiviert. Wenn der Kioskmodus deaktiviert ist, wird die Option **Öffentlicher Computer** auf der Portalseite nicht angezeigt und das Access Gateway bietet keine Kioskfunktionen.

Bei Computern, auf denen Java Virtual Machine (JVM) 1.5 oder höher installiert ist (wie Macintosh-, Windows 95- oder Windows 98-Computer), wird der Kioskmodus über ein Java-Applet bereitgestellt. Macintosh-Computer unterstützen nur dann den Kioskmodus, wenn Safari als Browser sowie JRE 1.5 installiert sind.

Wenn der Benutzer über den Kioskmodus angemeldet ist, sendet das Access Gateway nur Bilder (keine Daten) über die Verbindung. Auf diese Weise besteht kein Risiko, dass auf dem öffentlichen Computer temporäre Dateien oder Cookies zurückbleiben. Die temporären Dateien und die Cookies werden für den Zeitraum der Sitzung im Access Gateway gespeichert.

Der Browser verwendet standardmäßig eine Webadresse, die über das Administration Tool auf Gruppenbasis konfiguriert wurde. Das Webbrowserfenster kann auch Symbole für die Remotedesktop-, SSH-, Telnet 3270-Emulator-, Gaim-IM- und VNC-Clients enthalten. Die Symbole werden in der linken unteren Ecke des Fensters angezeigt. Die Angabe der Anwendungen erfolgt gruppenweise. Weitere Informationen zur Konfiguration von Anwendungen für den Kioskmodus finden Sie unter „Erstellen einer Kioskmodusressource“ auf Seite 160.

Das Webbrowserfenster bietet darüber hinaus Zugriff auf freigegebene Netzlaufwerke. Der Access Gateway-Administrator konfiguriert die gewährten Berechtigungen (nur Lesen oder Lesen/Schreiben) für jedes freigegebene Netzlaufwerk getrennt. Weitere Informationen zur Konfiguration der Netzwerkfreigaben finden Sie unter „Konfigurieren von Dateifreigaben für den Kioskmodus“ auf Seite 165.

Die Benutzer können Dateien von der Netzwerkfreigabe auf ihren Computer kopieren, indem sie die Datei einfach auf das KioskFTP-Symbol ziehen und im Dialogfeld **File Download** das Ziel auswählen.

Wichtig: Wenn Benutzer über den Kioskmodus angemeldet sind, werden Endpunktrichtlinien weder unterstützt noch durchgesetzt.

Der Kioskmodus umfasst die folgenden Anwendungen, sofern diese auf der Registerkarte **User Groups** im Administration Tool aktiviert wurden:

- Firefox-Webbrowser. Ob Firefox und die Standardwebadresse des Browsers enthalten sein sollen, wird auf Gruppenbasis konfiguriert. Firefox-Einstellungen, wie z. B. gespeicherte Kennwörter, werden für die nächste Sitzung beibehalten.
- Freigegebene Netzlaufwerke. Dies sind Symbole, die den Zugriff auf freigegebene Netzlaufwerke ermöglichen. Der Benutzer kann Dateien von einer Netzwerkfreigabe herunterladen, indem er die entsprechenden Dateien auf das KioskFTP-Symbol zieht (siehe „Konfigurieren von Dateifreigaben für den Kioskmodus“ auf Seite 165).
- Symbole für den Zugriff auf den VNC-Client, Remotedesktop, den Telnet 3270-Emulator und SSH: Die Clients, die in der Kiosksitzung enthalten sein sollen, konfigurieren Sie auf Gruppenbasis.

Weitere Informationen zur Verwendung der Clients finden Sie in den folgenden Abschnitten:

- „Remotedesktopclient“ auf Seite 162
- „SSH-Client“ auf Seite 163
- „Telnet 3270-Emulator-Client“ auf Seite 163
- „VNC-Client“ auf Seite 163
- „Instant Messaging“ auf Seite 164

Wenn der Browser der Benutzer für die Verwendung eines Proxyservers konfiguriert ist, verwenden die Benutzer, die im Kioskmodus verbunden sind, die Proxyeinstellung des Browsers.

Damit Benutzer über den Kioskmodus auf Unternehmensressourcen zugreifen können, muss dieser Modus zunächst aktiviert werden.

So aktivieren Sie den Kioskmodus:

Aktivieren Sie auf der Registerkarte **Global Cluster Policies** unter **Access options** die Option **Enable kiosk mode**.

Ist dieses Kontrollkästchen deaktiviert, können Benutzer den Kioskmodus nicht verwenden und die entsprechende Option ist auf der Webportalseite nicht verfügbar.

Bei aktiviertem Kioskmodus können Benutzer eine Verbindung über die Webportalseite herstellen.

So melden Sie sich unter Verwendung des Kioskmodus am Access Gateway an:

1. Stellen Sie über die Anmeldeseite eine Verbindung her (siehe „Herstellen einer Verbindung mit einer Webadresse“ auf Seite 152). Klicken Sie auf **Öffentlicher Computer**.

   Das **Citrix Secure Access**-Anmeldedialogfeld wird angezeigt.

2. Geben Sie Ihre Anmeldeinformationen ein und klicken Sie auf **Login**.

Hinweis: Benutzer, die im Kioskmodus angemeldet sind, können zum Herunterladen von Dateien aus dem Unternehmensnetzwerk das FTP-Protokoll verwenden. Dateien, die im Rahmen einer Kiosksitzung heruntergeladen wurden, können nicht an das Unternehmensnetzwerk zurückgesendet werden.

Erstellen einer Kioskmodusressource

Der Kioskmodus wird unter Verwendung der Kioskressourcen konfiguriert, die die Dateifreigaben und Anwendungen definieren, auf die die Benutzer beim Anmelden im Kioskmodus Zugriff haben. Standardmäßig ist der Kioskmodus deaktiviert. Zum Aktivieren des Kioskmodus müssen die Ressourcen konfiguriert und dann den Benutzergruppen hinzugefügt werden.

Der Kioskmodus wird auf der Registerkarte **Access Policy Manager** konfiguriert und dann den Gruppen im linken Bereich hinzugefügt.

Hinweis: Wenn der Benutzer bereits über einen allgemeinen Internetzugriff verfügt, bevor er eine Verbindung herstellt, kann der Benutzer über den Firefox-Browser im Webbrowserfenster das Internet durchsuchen, sofern keine Netzwerkressource definiert ist, die den Zugriff auf das Internet verweigert.

So erstellen und konfigurieren Sie eine Kioskressource:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **Kiosk Resources** und klicken Sie dann auf **New Kiosk Resource**.
3. Geben Sie einen Namen für die Ressource ein und klicken Sie auf **OK**.
4. Soll eine Dateifreigabe hinzugefügt werden, ziehen Sie die Ressource unter **File shares** auf **Shares**.
5. Wählen Sie die Anwendungen aus, auf die die Benutzer im Kioskmodus zugreifen können sollen.
6. Aktivieren Sie die Option **Save kiosk application settings**, um die Firefox-Grundeinstellungen zu speichern. Die Grundeinstellungen werden auf dem Remoteserver (der die Sitzung hostet) gespeichert. Klicken Sie auf **OK**.
7. Wenn Sie einer oder mehreren Gruppen eine Kioskressource hinzufügen möchten, klicken Sie auf die Ressource und ziehen Sie sie auf die Gruppe(n), für die die Richtlinie gilt.

Konfigurieren von Clientanwendungen für den Kioskmodus

Benutzern, die im Kioskmodus angemeldet sind, können Sie die Verwendung verschiedener Anwendungen erlauben, u. a.:

- Firefox-Webbrowser
- Remotedesktopclient
- SSH-Client
- Telnet 3270-Emulator-Client
- VNC-Client
- Instant Messaging

Diese Clientanwendungen können Sie auf der Registerkarte **Access Policy Manager** im Administration Tool konfigurieren.

So aktivieren Sie Clientanwendungen:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich unter **Kiosk Resources** auf eine Ressource und klicken Sie dann auf **Properties**.

   Soll Firefox aktiviert werden, geben Sie die Webadresse des Browsers ein.

   Wenn Remotedesktop aktiviert werden soll, geben Sie die IP-Adresse des Remotecomputers ein.
3. Wählen Sie unter **Kiosk resources** die Anwendungen aus, die die Benutzer verwenden können sollen. Klicken Sie auf **OK**.
4. Ziehen Sie die Ressource auf die Gruppe(n), zu der/denen sie gehört.

Firefox-Webbrowser

Mit dem Firefox-Webbrowser können Benutzer Verbindungen zum Internet herstellen, wenn sie im Kioskmodus angemeldet sind, und zwar auf dieselbe Weise, als würden sie an ihrem eigenen Computer sitzen.

So konfigurieren Sie Firefox:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich unter **Kiosk Resources** auf eine Ressource und klicken Sie dann auf **Properties**.
3. Aktivieren Sie **Enable Firefox** und geben Sie in das Textfeld die Adresse des Browsers ein.

Remotedesktopclient

Der Remotedesktopclient ermöglicht Benutzern den Remotezugriff auf den Desktop eines Servers, auf dem Windows-Terminaldienste ausgeführt werden. Für Remotedesktop ist keinerlei Konfiguration auf dem Benutzercomputer erforderlich.

Wenn Remotedesktop für den Kioskmodus konfiguriert ist, ist dies die einzige Anwendung, die vom Client verwendet werden kann. Sobald der Client eine Verbindung im Kioskmodus herstellt und die Remotedesktopverbindung startet, übernimmt Remotedesktop die Steuerung der Sitzung. Ein Umschalten zwischen Kiosk- und Remotedesktopsitzung ist nicht möglich. Wenn andere Clients, wie z. B. VNC oder SSH, konfiguriert sind, kann Remotedesktop nicht konfiguriert werden.

So konfigurieren Sie Remotedesktop:

1. Klicken Sie auf der Registerkarte **Access Policy Manager** mit der rechten Maustaste auf **Kiosk Resources**.
2. Geben Sie einen Namen für die Ressource ein und klicken Sie auf **OK**.
3. Aktivieren Sie **Remote Desktop** und geben Sie in das Textfeld den vollqualifizierten Domänennamen für den Server ein. Klicken Sie auf **OK**.

Remotedesktop bietet dem Benutzer uneingeschränkten Zugriff auf die Ressourcen eines Remotecomputers, beispielsweise auf Dateien, Anwendungen und Netzwerkressourcen. Auf diese Weise kann der Benutzer den Computer aus der Ferne so steuern, als würde er direkt vor ihm sitzen. Die Arbeit des Benutzers verbleibt auf dem Remotecomputer, d. h., es werden keine Dateien, sondern nur Bilder an den Computer des Benutzers gesendet.

Wenn sich Benutzer über einen öffentlichen Computer anmelden und Remotedesktop konfiguriert ist, können sie Remotedesktop über ein Symbol starten. Nach der Eingabe des Benutzernamens und des Kennworts wird der Desktop des Remotecomputers auf dem öffentlichen Computer angezeigt.

SSH-Client

Der SSH-Client ermöglicht es dem Benutzer, eine SSH-Verbindung zu einem Remotecomputer einzurichten.

So verwenden Sie den SSH-Client:

1. Wählen Sie auf der Portalseite die Option **Öffentlicher Computer** und melden Sie sich an.
2. Klicken Sie im Webbrowser auf das SSH-Symbol.
3. Geben Sie den Benutzernamen und den SSH-Hostnamen oder die IP-Adresse ein.

   Das SSH-Fenster wird geöffnet.

Telnet 3270-Emulator-Client

Der Telnet 3270-Emulator-Client ermöglicht es dem Benutzer, eine Telnet 3270-Verbindung zu einem Remotecomputer einzurichten.

So verwenden Sie den Telnet 3270-Emulator-Client:

1. Wählen Sie auf der Portalseite die Option **Öffentlicher Computer** und melden Sie sich an.
2. Klicken Sie im Webbrowser auf das Telnet 3270-Emulator-Symbol.

   Das x3270-Fenster wird geöffnet.
3. Wählen Sie im Menü **Connect** den Befehl **Other**.

   Das Fenster **x3270 Connect** wird geöffnet.
4. Geben Sie den Hostnamen oder die IP-Adresse ein und klicken Sie auf **Connect**, um sich anzumelden und eine Eingabeaufforderung zu erhalten.
5. Klicken Sie zum Anzeigen des 3270-Tastenfelds auf das Tastenfeldsymbol in der oberen rechten Ecke.

VNC-Client

Der VNC-Client ermöglicht Benutzern den Remotezugriff auf den Desktop eines VNC-Servers. Die Arbeit des Benutzers verbleibt auf dem Remoteserver, d. h., es werden keine Dateien, sondern nur Bilder an den Computer des Benutzers gesendet.

So verwenden Sie den VNC-Client:

1. Wählen Sie auf der Portalseite die Option **Öffentlicher Computer** und melden Sie sich an.
2. Klicken Sie im Webbrowser auf das VNC-Symbol.
3. Geben Sie in das Feld **VNC Host** die IP-Adresse des VNC-Hosts und in das Feld **Password** das Kennwort für den Server ein. Klicken Sie auf **Verbinden**.

   In einem Fenster auf Ihrem Computer wird der Desktop des VNC-Servers angezeigt.
4. Arbeiten Sie mit dem Remoteserver so, als wäre es Ihr lokaler Computer.

Hinweis: Wenn Sie Strg+Alt+Entf über den VNC-Server an den verbundenen Server senden möchten, drücken Sie **Umschalt+Strg+Alt+Entf**.

Instant Messaging

Gaim ist ein Instant-Messaging-Client, der die Verwendung mehrerer IM-Anwendungen unterstützt. Zu diesen Anwendungen gehören u.a.:

- AOL Instant Messenger
- ICQ (Oscar Protocol)
- MSN Messenger
- Yahoo! Messenger
- IRC

Gaim-Benutzer können sich gleichzeitig an mehreren Konten unterschiedlicher IM-Netzwerke anmelden.

So konfigurieren Sie Instant Messaging:

1. Wählen Sie auf der Anmeldeseite die Option **Öffentlicher Computer** und melden Sie sich an.
2. Doppelklicken Sie im Webbrowser auf das Gaim-Symbol.
3. Folgen Sie den Anweisungen in Gaim, um Instant Messaging-Anwendungen hinzuzufügen und die Anmeldung über diese Anwendungen vorzunehmen.

Konfigurieren von Dateifreigaben für den Kioskmodus

Wenn ein Benutzer eine Verbindung über einen Webbrowser herstellt und die Option **Öffentlicher Computer** wählt, öffnet das Access Gateway eine Kioskmodusverbindung. Falls Dateifreigaben konfiguriert sind, kann der Benutzer mit Dateien arbeiten, die sich in den Freigaben befinden. Die Dateien werden nicht auf den öffentlichen Computer heruntergeladen. Die für den Benutzer verfügbaren Netzwerkfreigaben werden auf der Registerkarte **Access Policy Manager** konfiguriert.

So erstellen Sie eine Dateifreigaberessource:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **File Share Resources**, klicken Sie dann auf **New File Share Resource**, geben Sie einen Namen ein und klicken Sie auf **OK**.
3. Geben Sie unter **Share source** den Pfad zur Freigabequelle wie folgt ein: *//Server/Freigabe*.
4. Wählen Sie unter **Mount type** das Dateifreigabe-Netzwerkprotokoll aus. Sie können dabei zwischen **CIFS/SMB** und **NFS** wählen.

Hinweis: CIFS/SMB (Common Internet File System/Server Message Block) ist das Netzwerkprotokoll, das in Microsoft Windows für die Dateifreigabe verwendet wird. NFS (Network File System) erlaubt es Ihnen, eine Diskpartition auf einem Remotecomputer so bereitzustellen (zu mounten), als ob sie sich auf der Festplatte des lokalen Computers befindet. NFS wird typischerweise auf Linux-Computern verwendet.

---

5. Wenn zum Bereitstellen eines CIFS/SMB-Laufwerks Administratorberechtigungen erforderlich sind, geben Sie unter **User name** den Benutzernamen und unter **Password** ein Kennwort ein. Bei Wahl von **NFS** sind diese Felder nicht aktiv.

   Alle Benutzer, die auf die Freigabe zugreifen, besitzen dieselben Rechte wie dieser Benutzer.
6. Geben Sie unter **Domain** die Active Directory-Domäne der Freigabe ein. Bei Wahl von **NFS** ist dieses Feld nicht aktiv.

7. Legen Sie unter **Permissions** fest, ob Remotebenutzern Lese- und Schreibrechte oder nur Leserechte für die Freigabe gewährt werden. Klicken Sie auf **OK**.

Hinweis: Zum Senden und Empfangen von Dateien kann das FTP-Protokoll verwendet werden.

Nach erfolgter Konfiguration muss die Dateifreigabe der Kioskressource hinzugefügt werden.

So fügen Sie einer Kioskressource eine Dateifreigabe hinzu:

1. Klicken Sie auf der Registerkarte **Access Policy Manager** im rechten Bereich unter **Kiosk Resources** mit der rechten Maustaste auf eine Ressource und klicken Sie dann auf **Properties**.
2. Wählen Sie eine Dateifreigabe unter **File Share Resources** aus und ziehen Sie sie in der Kioskressource unter **File Shares** auf **Shares**.
3. Klicken Sie auf **OK**.

So entfernen Sie eine Dateifreigabe:

Klicken Sie mit der rechten Maustaste im rechten Bereich der Registerkarte **Access Policy Manager** auf die Dateifreigabe und klicken Sie dann auf **Remove**.

Arbeiten mit Dateifreigaberessourcen

Sie können die freigegebenen Netzlaufwerke festlegen, auf die in den Sitzungen zugegriffen werden kann. Geben Sie dabei für jedes freigegebene Laufwerk an, ob Benutzer nur Lese- oder auch Schreibberechtigung besitzen sollen. Wenn Benutzern Lese- und Schreibrechte eingeräumt wurden, können diese die Dateien auf dem freigegebenen Netzlaufwerk ändern. Voraussetzung hierfür ist, dass das Konto des Benutzers die entsprechenden Berechtigungen besitzt.

So arbeiten Sie mit Dateifreigaberessourcen:

1. Doppelklicken Sie im Webbrowser auf das Symbol für ein freigegebenes Netzlaufwerk.

   Innerhalb des Kioskfensters wird das Freigabefenster geöffnet.
2. Ziehen Sie zum Kopieren einer Datei vom Netzlaufwerk auf Ihren Computer das Dateisymbol auf das KioskFTP-Symbol.
3. Navigieren Sie im Dialogfeld **Kiosk File Download** zu dem Speicherort, an den die Datei kopiert werden soll, und klicken Sie dann auf **Open**.

Nach Abschluss der FTP-Übertragung wird eine entsprechende Meldung angezeigt.

Die Übertragung von Ordnern oder das Zurückkopieren von Dateien auf das freigegebene Netzlaufwerk ist mit FTP nicht möglich.

Konfigurieren der Authentizierungsanforderungen nach einer Netzwerkunterbrechung

Wenn die Netzwerkverbindung eines Benutzers kurz unterbrochen wird, muss der Benutzer sich standardmäßig nicht neu anmelden, sobald die Verbindung wiederhergestellt ist. Sie können allerdings vorschreiben, dass Benutzer sich nach einer Unterbrechung doch neu anmelden müssen, z. B. wenn sich ein Computer im Ruhezustand oder Standby-Modus befunden hat, wenn der Benutzer in ein anderes drahtloses Netzwerk wechselt oder wenn eine Verbindung erzwungenermaßen beendet wurde.

So erzwingen Sie die Neuanmeldung von Benutzern nach einer Netzwerkunterbrechung oder einem Ruhezustand:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **General** unter **Session options** eine oder beide der folgenden Optionen:
   - **Authenticate after network interruption:** Bei Aktivierung dieser Option muss sich der Benutzer neu anmelden, wenn die Netzwerkverbindung kurz unterbrochen war.
   - **Authenticate upon system resume:** Bei Aktivierung dieser Option muss sich der Benutzer neu anmelden, wenn sich sein Computer im Standby-Modus oder Ruhezustand befunden hat. Diese Option bietet ein höheres Maß an Sicherheit für unbeaufsichtigte Computer.
4. Klicken Sie auf **OK**.

Hinweis: Wenn Sie eine Verbindung schließen und einen Benutzer oder eine Gruppe daran hindern möchten, automatisch wieder eine Verbindung herzustellen, müssen Sie die Einstellung **Authenticate after network interruption** aktivieren. Anderenfalls stellen die Benutzer unverzüglich eine neue Verbindung her, ohne dabei nach ihren Anmeldeinformationen gefragt zu werden.

Konfigurieren weiterer Gruppeneigenschaften

Mit zusätzlichen Gruppenrichtlinien können Sie den Zugriff der Benutzer auf das Netzwerk weiter konfigurieren:

- Aktivieren von IP-Pooling
- Aktivieren von Split DNS
- Aktivieren von internem Failover
- Aktivieren von Domänenanmeldeskripten
- Aktivieren von Secure Access Client-Sitzungstimeouts
- Konfigurieren von Websitzungstimeouts
- Deaktivieren von Desktopfreigaben

Aktivieren von IP-Pooling

Mitunter benötigen Benutzer, die sich über den Secure Access Client anmelden, eine eindeutige IP-Adresse für das Access Gateway. So muss z. B. in einer Samba-Umgebung jeder Benutzer, der eine Verbindung zu einem zugewiesenen Netzlaufwerk herstellt, den Eindruck erwecken, dass er sich von einer anderen IP-Adresse aus anmeldet. Wenn Sie das IP-Pooling für eine Gruppe aktivieren, kann das Access Gateway jedem Client einen eindeutigen IP-Adressalias zuweisen.

Sie können das Gatewaygerät angeben, das für das IP-Pooling verwendet werden soll. Als Gatewaygerät kommen sowohl das Access Gateway selbst als auch einige andere Geräte infrage. Wenn Sie kein Gateway festlegen, wird auf der Basis der Einstellungen auf der Registerkarte **General Networking** eine Access Gateway-Schnittstelle verwendet, wobei Folgendes gilt:

- Wenn Sie nur die Schnittstelle 0 konfiguriert haben (das Access Gateway befindet sich innerhalb Ihrer Firewall), wird die IP-Adresse der Schnittstelle 0 als Gateway verwendet.
- Wenn Sie die Schnittstellen 0 und 1 konfiguriert haben (das Access Gateway befindet sich in der DMZ), wird die IP-Adresse der Schnittstelle 1 als Gateway verwendet. In diesem Szenario ist Schnittstelle 1 die interne Schnittstelle.

Hinweis: Nach einer Aktualisierung von Access Gateway Version 4.9 oder 4.0 müssen die IP-Pooling-Daten erneut eingegeben werden.

So konfigurieren Sie IP-Pooling für eine Gruppe:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Benutzergruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **Network** die Option **Enable IP pools**.
4. Klicken Sie mit der rechten Maustaste unter **IP pool configuration** auf ein Gateway und klicken Sie dann auf **Change the IP Address Pool**.
5. Geben Sie unter **Starting IP Address** die erste IP-Adresse des Pools ein.
6. Geben Sie unter **Number of IP addresses** die Anzahl der IP-Adressaliasse ein. In allen IP-Pools können insgesamt bis zu 2000 IP-Adressen vorhanden sein.
7. Geben Sie unter **Default gateway** die IP-Adresse des Gateways ein.

   Wenn Sie dieses Feld leer lassen, wird ein Access Gateway-Netzwerk-adapter verwendet, wie dies bereits weiter oben in diesem Abschnitt beschrieben wurde. Wenn Sie ein anderes Gerät als Gateway festlegen, fügt das Access Gateway der Access Gateway-Routingtabelle einen Eintrag für diese Route hinzu.
8. Klicken Sie zweimal auf **OK**.

Aktivieren von Split DNS

Standardmäßig überprüft das Access Gateway lediglich das Remote-DNS des Benutzers. Durch Aktivieren von Split DNS können Sie Failoveroperationen auf das lokale DNS des Benutzers zulassen. Diese Einstellung kann im Dialogfeld **Verbindungseigenschaften** im Dialogfeld **Secure Access Client** außer Kraft gesetzt werden.

So aktivieren Sie Split DNS:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **Network** die Option **Enable split DNS**.

   Das Access Gateway führt lediglich dann eine Failoveroperation auf das lokale DNS durch, wenn kein Kontakt zu den angegebenen DNS-Servern hergestellt werden kann. Bei erfolgreicher Kontaktaufnahme, aber negativer Antwort erfolgt kein Failover. Klicken Sie auf **OK**.

Aktivieren von internem Failover

Durch die Konfiguration der lokalen DNS-Einstellungen für den Client ist der Secure Access Client in der Lage, durch eine Firewall hindurch eine Verbindung zum Access Gateway herzustellen. Wenn diese Einstellungen konfiguriert sind, führt der Client ein Failover zur internen IP-Adresse des Access Gateways durch, falls die externe IP-Adresse nicht erreichbar ist.

So aktivieren Sie das interne Failover:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Aktivieren Sie unter **Advanced options** die Option **Enable internal failover**.

Wenn dieses Kontrollkästchen aktiviert ist, wird die interne IP-Adresse des Access Gateway in die Failoverliste aufgenommen. Falls Sie externen Administratorzugriff deaktiviert haben, steht Port 9001 nicht zur Verfügung. Soll eine Verbindung zu Port 9001 hergestellt werden, wenn Sie sich über eine externe Verbindung anmelden, konfigurieren Sie die IP-Pools und stellen Sie die Verbindung zur niedrigsten IP-Adresse im IP-Pool her.

Aktivieren von Domänenanmeldeskripten

Im Netzwerk sind ggf. Anmeldeskripte vorhanden, die nach einer erfolgreichen Anmeldung auf dem Clientcomputer ausgeführt werden. Wenn auf dem Access Gateway Anmeldeskripte aktiviert sind, richtet das Access Gateway nach der Authentifizierung die Verbindung ein, ruft die Windows-Anmeldeskripte vom Domänencontroller ab und führt diese aus, um Operationen wie die automatische Laufwerkszuordnung auszuführen.

Hinweis: Voraussetzung dafür, dass Clients die Single Sign-On-Funktion unter Windows sowie die Anmeldeskripte verwenden können, ist die Anmeldung als Hauptbenutzer oder die Mitgliedschaft in der Gruppe der Hauptbenutzer.

Das Access Gateway kann Anmeldeskripte ausführen, die im Windows-Profil des Benutzers bzw. in einer Active Directory-Gruppenrichtlinie definiert sind.

Wenn kein Kontakt zum Domänencontroller hergestellt werden kann, wird zwar die Access Gateway-Verbindung hergestellt, die Anmeldeskripte werden aber nicht ausgeführt.

Wichtig: Die Clientarbeitsstation muss ein Mitglied der Domäne sein, damit Domänenanmeldeskripte ausgeführt werden können.

So aktivieren Sie Anmeldeskripte:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **General** unter **Session options** die Option **Run logon scripts**. Klicken Sie auf **OK**.

Hinweis: Die Anmeldeskriptunterstützung ist beschränkt auf Skripte, die von der Befehlsverarbeitung ausgeführt werden, wie z. B. EXE- und BAT-Dateien. Visual Basic- und JavaScript-Anmeldeskripte werden nicht unterstützt.

Aktivieren von Secure Access Client-Sitzungstimeouts

Sie können den Secure Access Client so konfigurieren, dass die Trennung der Verbindung zum Access Gateway erzwungen wird, falls während eines bestimmten Zeitraums (in Minuten) keinerlei Aktivitäten über die Verbindung zu verzeichnen sind. Eine Minute vor dem Timeout (also der Trennung) der Sitzung erhält der Benutzer eine Warnmeldung, dass die Sitzung in Kürze geschlossen wird. Falls die Sitzung tatsächlich geschlossen wird, muss der Benutzer sich erneut anmelden.

Beim Konfigurieren eines Werts für ein Sitzungstimeout stehen drei Optionen zur Auswahl:

- **User session timeout:** Mit dieser Einstellung trennt der Secure Access Client die Verbindung nach Ablauf der Timeoutfrist, unabhängig von den aktuellen Aktivitäten des Benutzers. Der Benutzer hat keine Möglichkeit, diese Trennung nach Ablauf der Timeoutfrist zu vermeiden.
- **Network inactivity timeout:** Mit dieser Einstellung trennt der Secure Access Client die Verbindung, wenn während des angegebenen Zeitraums keine Netzwerkpakete mehr vom Client an das Access Gateway gesendet werden.
- **Idle session timeout:** Mit dieser Einstellung wird die Benutzersitzung beendet, wenn während des angegebenen Zeitraums die Maus oder die Tastatur nicht mehr benutzt werden.

Zum Aktivieren dieser Einstellungen geben Sie jeweils den Zeitraum in Minuten für die Timeoutfrist ein (zulässige Werte: 1 bis 65536). Mit dem Wert Null (0) deaktivieren Sie die jeweilige Einstellung. Wenn Sie den Wert 0 eingeben, wird das Sitzungstimeout nicht aktiviert und die Einstellung wirkt sich nicht auf Clientverbindungen aus.

Falls Sie mehrere Einstellungen gleichzeitig aktivieren, wird die Clientverbindung geschlossen, sobald die erste Timeoutfrist abläuft.

So aktivieren Sie Sitzungstimeouts:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Geben Sie auf der Registerkarte **General** unter **Session options** den Zeitraum in Minuten für die folgenden Einstellungen ein:
   - **User session timeout**
   - **Network inactivity timeout**
   - **Idle session timeout**
4. Klicken Sie auf **OK**.

Konfigurieren von Websitzungstimeouts

Wenn ein Benutzer beim Access Gateway angemeldet ist und über einen Webbrowser eine Verbindung zu Websites im sicheren Netzwerk herstellt, werden Cookies gespeichert, mit denen ermittelt wird, ob die Websitzung des Benutzers auf dem Access Gateway noch aktiv ist. Wenn das Access Gateway-Cookie abläuft und die Authentifizierung über die Anmeldeseite aktiviert ist, wird der Benutzer aufgefordert, die Authentifizierungsinformationen einzugeben, damit er die Websitzung wieder aufnehmen kann. Damit wird der Zeitraum beschränkt, in dem Netzwerkangriffe über eine unbeaufsichtigte Websitzung erfolgen könnten, sodass ein gewisser Grad an Sicherheit entsteht.

So aktivieren Sie das Websitzungstimeout:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Geben Sie unter **Access options** den Zeitraum in Minuten in das Feld **Web session time-out** ein.

   Soll das Websitzungstimeout deaktiviert werden, geben Sie den Wert **0** in das Textfeld ein.
3. Klicken Sie auf **Submit**.

Deaktivieren von Desktopfreigaben

Der Secure Access Client bietet eine Funktion für die Desktopfreigabe. Ein Benutzer kann im Infobereich von Windows mit der rechten Maustaste auf das Secure Access Client-Symbol klicken und die Option **Desktop freigeben** wählen. Mit dieser Option wird eine Liste aller anderen Benutzer aufgerufen, die über einen Secure Access Client beim Access Gateway angemeldet sind.

In einigen Unternehmen kann diese Funktion zu Bedenken im Hinblick auf den Datenschutz führen, weil jeder Benutzer, der über den Secure Access Client angemeldet ist, eine Liste mit allen derzeit angemeldeten Benutzern sehen kann.

Soll die Liste der Onlinebenutzer für eine bestimmte Benutzergruppe nicht sichtbar sein, können Sie die Funktion zur Desktopfreigabe für diese Access Gateway-Benutzergruppe deaktivieren.

Beim Deaktivieren der Desktopfreigabe für eine Benutzergruppe gilt Folgendes:

- Klickt ein Mitglied dieser Benutzergruppe mit der rechten Maustaste auf das Secure Access Client-Symbol im Infobereich von Windows, wird die Option **Desktop freigeben** nicht im Menü angezeigt. Die Benutzer in dieser Gruppe können über das Secure Access Client-Symbol keine Liste der anderen Onlinebenutzer abrufen (und auch nicht die Funktion für die Desktopfreigabe verwenden).
- Die Mitglieder dieser Benutzergruppe werden nicht in der Onlineliste der anderen Benutzer aufgeführt, für die die Desktopfreigabe aktiviert ist.

So deaktivieren Sie die Desktopfreigabe:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Aktivieren Sie auf der Registerkarte **General** unter **Application options** die Option **Disable desktop sharing**. Klicken Sie auf **OK**.

Schließen und Deaktivieren von Benutzerverbindungen

Mit dem Real-time Monitor werden die offenen VPN-Verbindungen nach Benutzername und MAC-Adresse geordnet aufgelistet. Für jeden Benutzer wird auch der Verbindungstyp nach Protokoll (wie z. B. TCP oder UDP) geordnet angezeigt. Zusätzliche Informationen zur Verbindung können den Angaben zur Ziel-IP-Adresse und zum Zielport entnommen werden. Bei Verbindungen zum Port 21 handelt es sich z. B. um FTP-Verbindungen, während Verbindungen zum Port 23 Telnet-Verbindungen sind.

Die Verbindungen können wie folgt verwaltet werden:

- Sie können Verbindungen, z. B. TCP- oder UDP-Verbindungen, schließen.

  Nehmen wir z. B. an, dass ein Benutzer eine TCP-Verbindung zu einer Ziel-IP-Adresse (vielleicht einem zugeordneten Laufwerk) besitzt, auf die der Benutzer eigentlich nicht zugreifen können soll. Sie können in diesem Fall die Zugriffssteuerungsliste für die Gruppe korrigieren, der dieser Benutzer angehört, und dann die TCP-Verbindung schließen. Weitere Informationen zur Verwaltung von Zugriffssteuerungslisten finden Sie unter „Konfigurieren lokaler Benutzer“ auf Seite 84. Wenn Sie die Zugriffssteuerungsliste nicht vor dem Schließen der Verbindung korrigieren, kann der Benutzer die TCP-Verbindung erneut einrichten.

  Hinweis: Das Access Gateway behält Verbindungen zur Ziel-IP-Adresse 0.0.0.0 bei, die für VPN-Operationen erforderlich sind. Durch Schließen einer dieser Verbindungen werden aktive Verbindungen vorübergehend geschlossen.

- Sie können die Verbindung eines Benutzers deaktivieren und nachfolgende Anmeldungen durch diesen Benutzer an der aufgeführten MAC-Adresse verhindern. Der Benutzer kann sich dann von einer anderen MAC-Adresse aus anmelden.
- Sie können eine Kombination aus Benutzername/MAC-Adresse erneut aktivieren.

Verarbeitung von Verbindungen im Access Gateway

Wenn ein Benutzer plötzlich die Verbindung zum Netzwerk trennt oder den Computer in den Ruhezustand oder Standby-Modus versetzt, wird die Verbindung zum Access Gateway nach 10 Minuten getrennt.

Aufgrund dieses Verhaltens ist Folgendes zu beachten:

- Es kann passieren, dass der Benutzer im Access Gateway Real-time Monitor weitere 10 Minuten lang als aktiv angezeigt wird. Erst danach wird die Verbindung getrennt.
- Der inaktive Benutzer belegt so lange eine Lizenz, bis diese Wartezeit abgelaufen und die Verbindung geschlossen ist. Wird eine Verbindung getrennt, wird die Lizenz nach 30 Sekunden freigegeben.

Diese Wartezeit gilt nicht bei Verbindungen, die über den Real-time Monitor getrennt werden.

Schließen einer Verbindung zu einer Ressource

Sie können die Verbindung eines Benutzers mit einer bestimmten Ressource vorübergehend schließen, ohne dessen Verbindung zu unterbrechen. Um zu verhindern, dass der Benutzer wieder eine Verbindung zur Ressource herstellt, sollten Sie die Zugriffssteuerungsliste der Gruppe korrigieren, der der Benutzer angehört.

So schließen Sie eine Verbindung:

1. Klicken Sie im Administration Desktop auf das Symbol für den Citrix Real-time Monitor.
2. Klicken Sie auf den Pfeil, um den Eintrag für den Benutzer zu erweitern.
3. Klicken Sie mit der rechten Maustaste auf die Verbindung, die Sie schließen möchten, und wählen Sie dann **Close connection**.

Deaktivieren und Aktivieren eines Benutzers

Das Access Gateway verfolgt Benutzerverbindungen anhand einer Kombination aus Benutzername und MAC-Adresse, sodass ein Benutzer gleichzeitige Verbindungen von verschiedenen Computern aus einrichten kann. Sie können eine Kombination aus Benutzername und MAC-Adresse deaktivieren und aktivieren. Durch Deaktivieren eines Benutzers wird eine Lizenz frei.

So deaktivieren Sie einen Benutzer an einer bestimmten MAC-Adresse:

1. Klicken Sie im Administration Desktop auf das Symbol für den Citrix Real-time Monitor.
2. Klicken Sie mit der rechten Maustaste auf den Haupteintrag für den Benutzer und wählen Sie **Disable User from MAC**.

Der Benutzer kann so lange keine Verbindung von dieser MAC-Adresse aus einrichten, bis Sie den Benutzer wieder aktivieren oder das Access Gateway neu starten.

So aktivieren Sie einen Benutzer an einer bestimmten MAC-Adresse:

1. Klicken Sie im Administration Desktop auf das Symbol für den Citrix Real-time Monitor.
2. Klicken Sie mit der rechten Maustaste auf den Eintrag für den Benutzer und wählen Sie **Enable User from MAC**.

   Der Benutzer kann jetzt eine Verbindung einrichten, sofern eine Lizenz verfügbar ist.

Anfordern von Clientzertifikaten für die Authentifizierung

Wenn Sie auf eine zusätzliche Authentifizierung Wert legen, können Sie das Access Gateway so konfigurieren, dass Clientzertifikate zur Authentifizierung angefordert werden.

Das Access Gateway kann Clientzertifikate in den folgenden Speicherorten authentifizieren:

- Im Zertifikatspeicher des Windows-Betriebssystems auf einem Clientcomputer. In diesem Fall wird das Zertifikat unter Verwendung der Microsoft Management Console (MMC) separat im Zertifikatspeicher installiert.
- Auf einer Smartcard oder einem Hardwaretoken. In diesem Fall ist das Zertifikat in die Smartcard eingebettet und wird über einen Smartcardleser eingelesen, der mit dem Netzwerk verbunden ist.

Hinweis: Die Konfiguration des Access Gateways bleibt gleich, unabhängig davon, ob die Zertifikate im Windows-Betriebssystem oder auf einer Smartcard gespeichert sind. Zur Unterstützung von Clientzertifikaten, die sich an diesen Speicherorten befinden, ist keine besondere Konfiguration erforderlich.

Wenn Clients im Kioskmodus oder von einem Linux-Computer aus eine Verbindung herstellen, werden clientseitige Zertifikate nicht unterstützt. Falls im Access Gateway Clientzertifikate aktiviert sind, funktionieren Linux-Clients und der Kioskmodus nicht.

Wenn Sie das Access Gateway so konfigurieren, dass Clientzertifikate angefordert werden, müssen alle Benutzer, die sich über das Access Gateway anmelden, ein sicheres Clientzertifikat vorlegen. Das Zertifikat kann daher aus dem Zertifikatspeicher in Windows oder von einer Smartcard stammen.

So legen Sie fest, dass Clientzertifikate erforderlich sein sollen:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Aktivieren Sie unter **Select security options** die Option **Require secure client certificates**.
3. Klicken Sie auf **Submit**.

Definieren von Clientzertifikatskriterien

Verwenden Sie zum Festlegen der Kriterien, die die Clientzertifikate erfüllen müssen, einen booleschen Ausdruck. Damit der Benutzer einer Gruppe angehören kann, muss er nicht nur alle anderen für die jeweilige Gruppe konfigurierten Authentifizierungsregeln einhalten, sondern auch die Zertifikatskriterien erfüllen. So erfordern z. B. die folgenden Kriterien, dass im Betreff-Feld des vom jeweiligen Benutzer bereitgestellten Clientzertifikats für die Organisationseinheit (Organizational Unit, OU) *Buchhaltung* und für den gemeinsamen Namen (Common Name, CN) ein Wert festgelegt ist, der mit dem lokalen Benutzernamen des Benutzers auf dem Access Gateway übereinstimmt.

client_cert_end_user_subject_organizational_unit="Buchhaltung" und username=client_cert_end_user_subject_common_name.

Folgende Operatoren können verwendet werden:

and logisches UND

= Übereinstimmungsprüfung

Gültige Konstanten für die Kriterien:

true logisches WAHR

Gültige Variablen für die Kriterien:

user name lokaler Benutzername auf dem Access Gateway
client_cert_end_user_subject_common_name CN-Attribut des Betreffs des Clientzertifikats
client_cert_end_user_subject_organizational_unit OU-Attribut des Betreffs des Clientzertifikats
client_cert_end_user_subject_organization O-Attribut des Betreffs des Clientzertifikats

Die Werte für die Clientzertifikatskriterien müssen in Anführungszeichen gesetzt werden. Beispiele für richtige und falsche Schreibweise:

Der boolesche Ausdruck *client_cert_end_user_subject_common_name="clients.gateways.citrix.com"* ist gültig und funktioniert.

Der boolesche Ausdruck *client_cert_end_user_subject_common_name=clients.gateways.citrix.com* ist ungültig und funktioniert nicht.

So legen Sie die Clientzertifikatskonfiguration fest:

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** auf eine andere Gruppe als die Standardgruppe und klicken Sie dann auf **Properties**.

   Hinweis: Für die Standardbenutzergruppe ist die Clientzertifikatskonfiguration nicht verfügbar.

2. Geben Sie auf der Registerkarte **Client Certificate** unter **Client certificate criteria expression** die Zertifikatsinformationen ein. Klicken Sie auf **OK**.

Verwenden von Clientzertifikaten mit Access Gateway Advanced Edition

Sowohl für das Access Gateway als auch für die Server, auf denen Advanced Edition ausgeführt wird, kann die Verwendung sicherer Clientzertifikate angefordert werden. Beachten Sie die folgenden Hinweise beim Konfigurieren der Verwendung von Clientzertifikaten:

- Der Secure Access Client kann Zertifikate aus dem Windows-Benutzerprofil, von einer Smartcard oder einem Hardwaretoken lesen, das die Microsoft Crypto-API unterstützt.
- Das Clientzertifikat stellt keine Authentifizierung des Benutzers dar, sondern fungiert lediglich als zusätzliche Clientbedingung, z. B. ein Endpunktscan. Die Benutzer müssen nach wie vor ihr Kennwort oder ihren Tokencode eingeben.
- Wenn das Access Gateway so konfiguriert ist, dass Clientzertifikate angefordert werden, kann das Access Gateway über die Citrix Presentation Server Clients keine direkten Verbindungen mehr zu Citrix Presentation Server herstellen. Der Secure Access Client muss ICA-Verbindungen über das Access Gateway herstellen.

Installieren von Stammzertifikaten

Auf allen Clientgeräten, die über das Access Gateway eine Verbindung zum sicheren Netzwerk herstellen, muss ein Stammzertifikat vorliegen.

Das Windows-Betriebssystem und Internet Explorer unterstützen bereits die meisten vertrauenswürdigen Stammzertifizierungsstellen. Bei diesen Zertifizierungsstellen ist es also nicht nötig, Stammzertifikate abzurufen und auf dem Clientgerät zu installieren. Wenn Sie jedoch eine andere Zertifizierungsstelle verwenden, müssen Sie die entsprechenden Stammzertifikate selbst abrufen und installieren.

Abrufen eines Stammzertifikats von einer Zertifizierungsstelle

Stammzertifikate sind bei denselben Zertifizierungsstellen erhältlich wie Serverzertifikate. Bekannte und vertrauenswürdige Zertifizierungsstellen sind beispielsweise Verisign, Baltimore, Entrust und die jeweils angeschlossenen Unternehmen.

Bei den Zertifizierungsstellen wird in der Regel vorausgesetzt, dass Sie bereits über geeignete Stammzertifikate verfügen. (Die meisten Webbrowser enthalten Stammzertifikate.) Wenn Sie jedoch Zertifikate von einer Zertifizierungsstelle heranziehen, die auf dem Clientcomputer noch nicht genutzt wird, müssen Sie das Stammzertifikat explizit anfordern.

Es stehen mehrere Arten von Stammzertifikaten zur Auswahl. VeriSign bietet beispielsweise rund 12 Stammzertifikate für verschiedene Zwecke an. Achten Sie also darauf, das jeweils richtige Stammzertifikat bei der Zertifizierungsstelle abzurufen.

Installieren von Stammzertifikaten auf einem Clientgerät

Stammzertifikate werden mit der Microsoft Management Console (MMC) unter Windows installiert. Hierbei kommt der Zertifikatsimport-Assistent zum Einsatz. Das Zertifikat wird unter den vertrauenswürdigen Stammzertifizierungsstellen für den lokalen Computer gespeichert.

Weitere Informationen zur Verfügbarkeit von Stammzertifikaten und zu deren Installation auf anderen Plattformen außer 32-Bit-Windows finden Sie in der Produktdokumentation für das jeweils verwendete Betriebssystem.

Auswählen einer Verschlüsselungsart für Clientverbindungen

Die gesamte Kommunikation zwischen dem Secure Access Client und dem Access Gateway wird mit SSL verschlüsselt. Mit dem SSL-Protokoll sind zwei Computer in der Lage, Verschlüsselungssammlungen für die symmetrische Verschlüsselung von Daten über eine sichere Verbindung auszuhandeln.

Sie können die Verschlüsselungssammlung festlegen, die das Access Gateway für die symmetrische Datenverschlüsselung bei einer SSL-Verbindung verwendet. Die Auswahl einer starken Verschlüsselungssammlung senkt die Gefahr böswilliger Angriffe. Je nach den Sicherheitsrichtlinien Ihres Unternehmens müssen Sie außerdem ggf. eine bestimmte Verschlüsselungssammlung für die symmetrische Verschlüsselung über sichere Verbindungen festlegen.

Hinweis: Wenn Sie über das Access Gateway Zugriff auf Citrix Presentation Server bereitstellen, wird auch der ICA-Datenverkehr an das Access Gateway mit diesen Verschlüsselungssammlungen verschlüsselt.

Für SSL-Verbindungen stehen RC4-, 3DES- und AES-Verschlüsselungssammlungen zur Auswahl. Die Standardeinstellung lautet RC4 128-Bit. Der MD5- oder SHA-Hash-Algorithmus wird zwischen dem Client und dem Server ausgehandelt.

Bei der Verschlüsselung sicherer Verbindungen mit öffentlichem Schlüssel wird RSA verwendet. Für die symmetrische Verschlüsselung stehen dabei die folgenden Verschlüsselungssammlungen und Hash-Algorithmen bereit:

- RC4 128-Bit, MD5/SHA
- 3DES, SHA
- AES 128/256-Bit, SHA

So wählen Sie eine Verschlüsselungsart für Clientverbindungen aus:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie unter **Select security options** im Feld **Select encryption type for client connections** die gewünschte Verschlüsselungssammlung für sichere Verbindungen aus. Klicken Sie auf **Submit**.

Unterstützung von VoIP-Softphones

Echtzeitanwendungen wie Sprach- oder Videoanwendungen werden über UDP implementiert, da TCP aufgrund der Verzögerungen durch Quittierungen und erneute Übertragung verlorener Pakete für Echtzeitverkehr nicht geeignet ist. Bei diesen Anwendungen ist es wichtiger, die Pakete in Echtzeit zu liefern, als sicherzustellen, dass alle Pakete ihr Ziel erreichen. Diese Echtzeitleistung lässt sich mit keinen der auf TCP basierenden Tunnelverfahren erreichen.

Das Access Gateway umgeht dieses Problem, indem UDP-Pakete als spezielle IP-Pakete, die keiner TCP-Quittierung bedürfen, über den sicheren Tunnel geroutet werden. Selbst wenn die Pakete im Netzwerk verloren gehen, wird weder vom Client noch von den Serveranwendungen versucht, diese Pakete wiederherzustellen. Auf diese Weise lässt sich auch über einen sicheren Tunnel auf TCP-Basis eine (UDP-artige) Echtzeitperformance erreichen.

Wenn das Access Gateway als eigenständiges Gerät installiert ist und Benutzer eine Verbindung über den Secure Access Client herstellen, wird die bidirektionale Kommunikation mit den folgenden VoIP-Softphones (Voice over IP) unterstützt:

- Avaya IP Softphone
- Nortel IP Softphone
- Cisco IP Softphone
- Cisco IP Communicator

Zwischen der IP-Nebenstellenanlage des Herstellers und der Softphone-Software auf dem Clientcomputer werden sichere Tunnel unterstützt. Damit der VoIP-Verkehr den sicheren Tunnel durchqueren kann, muss der Secure Access Client und eines der oben genannten Softphones auf demselben System installiert sein. Beim Tunneln des VoIP-Verkehrs über den sicheren Tunnel werden die folgenden Softphonefunktionen unterstützt:

- Ausgehende Anrufe vom IP-Softphone
- Eingehende Anrufe an das IP-Softphone
- Bidirektionaler Datenverkehr

Verbessern von VoIP-Verbindungen

VoIP-Verkehr wird über das UDP-Protokoll transportiert. Diese Art von Verkehr reagiert sehr empfindlich auf Latenzprobleme. Das Access Gateway tunnelt den UDP-Verkehr über SSL-Verbindungen. Wenn es in der VoIP-Anwendung zu Latenz kommt, können Sie mit der Einstellung **Improve latency for Voice Over IP traffic** die Latenz minimieren und die Audioqualität erhöhen.

Bei dieser Einstellung greift das Access Gateway auf schwächere Verschlüsselungssammlungen zurück (56-Bit). Diese schwächeren Verschlüsselungssammlungen werden nicht nur für den VoIP-Verkehr verwendet, sondern für den gesamten Datenverkehr, der über das UDP-Protokoll übertragen wird. Bevor Sie diese Option aktivieren, sollten Sie die Auswirkungen auf die Sicherheit bedenken, die diese schwächeren Verschlüsselungssammlungen für die Verschlüsselung des UDP-Datenverkehrs mit sich bringen.

Folgende Verschlüsselungssammlungen werden zur Verschlüsselung des UDP-Datenverkehrs verwendet:

- RSA EXP 1024, RC4 56 Bit, MD5
- RSA EXP 1024, RC4 56 Bit, SHA

Hinweis: Wenn Sie die Einstellung **Improve latency for Voice Over IP traffic** nicht aktivieren, wird der UDP-Datenverkehr mit der Verschlüsselungssammlung für die symmetrische Verschlüsselung verschlüsselt, die unter der Einstellung **Select encryption type for client connections** auf der Registerkarte **Global Cluster Policies** festgelegt ist.

Die Verschlüsselungssammlungen werden zwischen dem Client und dem Access Gateway in der aufgeführten Reihenfolge ausgehandelt. Die erste akzeptierte Methode wird für die Sitzung verwendet.

So verbessern Sie die Latenz für UDP-Verkehr:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Aktivieren Sie unter **Select security options** die Option **Improve latency for Voice Over IP traffic**.
3. Zum Festlegen einer Verschlüsselungssammlung klicken Sie zunächst auf **Select encryption type for client connections** und wählen Sie dann die gewünschte Verschlüsselungssammlung aus. Klicken Sie auf **Submit**.

Konfigurieren der Anmelde- und Portalseiten für den Secure Access Client

Das Access Gateway kann so konfiguriert werden, dass Benutzer die Anmeldeseite und die Portalseite verwenden. Auf der Anmeldeseite müssen Benutzer erst ihre Anmeldeinformationen eingeben und werden dann mit der Portalseite verbunden, auf der sich Benutzer mit dem Secure Access Client oder Kioskmodus anmelden können.

Konfigurieren der Access Gateway-Anmeldeseiten

Auf der Access Gateway-Anmeldeseite müssen sich Benutzer erst anmelden, bevor sie mit dem Secure Access Client oder dem Kioskmodus eine Verbindung herstellen. Sie haben die Wahl zwischen der Standardanmeldeseite, die Teil des Access Gateways ist, oder Sie können die Anmeldeseite mit Ihrem Firmenlogo, einem Cascading Stylesheet und HTML-Fußzeilentext, den Sie selbst verfassen, anpassen.

Aktivieren der Anmeldeseitenauthentifizierung

Standardmäßig muss sich ein Benutzer an der Anmeldeseite und dann am Secure Access Client oder im Kioskmodus anmelden. Mit den folgenden beiden Methoden erreichen Sie, dass die Anmeldung an der Anmeldeseite entfällt:

- Sie können eine globale Richtlinie einrichten, mit der die Authentifizierung für die Anmeldeseite deaktiviert wird und die angibt, welche Anmeldeseite für alle Benutzer angezeigt wird. Diese globale Richtlinie setzt alle Anmeldeseitenfestlegungen für Gruppen außer Kraft.
- Sie können Ihre Website direkt mit Links zum Secure Access Client und zum Kioskmodus versehen (siehe dazu „Einfügen von Links zu Clients auf Ihrer Website“ auf Seite 189).

So aktivieren Sie die Anmeldeseitenauthentifizierung:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie unter **Advanced options** die Option **Enable logon page authentication**.
3. Klicken Sie auf **Submit**.

Wenn das Kontrollkästchen **Enable logon page authentication** nicht aktiviert ist, meldet sich der Benutzer nicht an, sondern er wird direkt zur benutzerdefinierten Portalseite weitergeleitet.

Anpassen der Anmeldeseite

Sie passen die Anmeldeseite an, indem Sie eigene Bilder hochladen, Stylesheets und Text verwenden. Nach dem Upload wird den Benutzern die angepasste Anmeldeseite anstelle der Standardseite angezeigt.

So passen Sie die Anmeldeseite auf dem Access Gateway an:

1. Klicken Sie auf die Registerkarte **Portal Page Configuration**.
2. Wählen Sie auf der Registerkarte **Logon Page** in der Dropdownliste **Logon Page Type** die Option **Customized Logon Page** aus.
3. Wenn Sie eine angepasste Portalseite installieren, führen Sie die entsprechenden unten beschriebenen Tasks aus:
    - Um ein Bild hochzuladen, klicken Sie unter **Primary Logo Image** auf **Upload new primary image**, wählen Sie die Bilddatei aus und klicken Sie dann auf **Öffnen**.
    - Um eine weitere Bilddatei hochzuladen, klicken Sie unter **Secondary Logo Image** auf **Upload new secondary image**.
    - Wenn Sie ein Stylesheet verwenden, können Sie unter **Stylesheet** entweder das aktuelle Stylesheet herunterladen oder ein neues Stylesheet hochladen.
    - Um eine Fußzeile zu erstellen, geben Sie im Bereich **HTML footer** den Text ein und klicken Sie dann im oberen Bereich der Seite auf **Apply**.

Wählen Sie nach der Installation der angepassten Portalseite die Portalseite für die Benutzer aus. Weitere Informationen finden Sie an folgenden Stellen:

- Informationen zur Verwendung der Portalseite, die Teil des Geräts ist, finden Sie unter „Access Gateway-Portalseitenvorlagen“ auf Seite 185.
- Informationen, wie Sie Benutzern die Wahl überlassen, ob sie sich mit dem Secure Access Client, dem Webinterface oder dem Kioskmodus (falls aktiviert) anmelden, finden Sie unter „Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen“ auf Seite 190.
- Informationen darüber, ob Benutzer mehr als einen Authentifizierungstyp bei der Anmeldung verwenden müssen, finden Sie unter „Anmelden mit Zweimethodenauthentifizierung“ auf Seite 191.
- Informationen darüber, ob eine Vorauthentifizierungsrichtlinie konfiguriert ist, finden Sie unter „Anmelden, wenn Vorauthentifizierungsrichtlinien konfiguriert sind“ auf Seite 192.

Access Gateway-Portalseitenvorlagen

Wenn ein Benutzer den Secure Access Client über einen Webbrowser startet, wird Benutzern die Anmeldeseite Citrix Access Gateway angezeigt. Nachdem sich Benutzer angemeldet haben, werden Sie an eine Portalseite weitergeleitet, auf der sie die Wahl haben, sich mit dem Secure Access Client oder im Kioskmodus anzumelden.

Citrix stellt Portalseitenvorlagen zur Verfügung, die individuell angepasst werden können. Eine einfache Form der Anpassung der Standardportalseite ist das Ersetzen des Logos.

Der Text für **Eigener Computer** und **Öffentlicher Computer** verwendet eine Variable, über die der Text in die Vorlage eingefügt werden kann. Der Text in diesen beiden Abschnitten kann nicht geändert werden.

Eine dieser Vorlagen enthält Links zum Secure Access Client und zum Kioskmodus. Die anderen beiden Vorlagen enthalten Links zu jeweils nur einer Anmeldemethode. Ausschlaggebend für die Wahl einer Vorlage sind die Zugriffsrechte, die Sie der jeweiligen Gruppe gewähren möchten. So kann es z. B. vorkommen, dass Sie einigen Benutzern den Zugriff auf beide Clients gestatten möchten, während andere Benutzer nur auf den Secure Access Client oder den Kioskmodus zugreifen können sollen. Fügen Sie dem Access Gateway dazu benutzerdefinierte Portalseiten hinzu und legen Sie dann fest, welche Portalseite für welche Benutzergruppe verwendet werden soll.

Hinweis: Wenn Sie der Vorlage Text hinzufügen oder Formatänderungen vornehmen möchten, sollten Sie jemanden zurate ziehen, der sich mit HTML auskennt. Änderungen, die über die Möglichkeiten hinausgehen, die in diesem Abschnitt beschrieben werden, werden nicht unterstützt.

Herunterladen von und Arbeiten mit Portalseitenvorlagen

Die Portalseitenvorlagen stehen im Administration Portal auf der Seite **Downloads** zur Verfügung.

Die Portalseitenvorlagen enthalten Variablen, die das Access Gateway durch den aktuellen Benutzernamen und durch Links ersetzt, die für den Computer relevant sind, der die Verbindung herstellt (Windows 2000 oder höher oder Linux).

Wenn Sie auch Benutzer mit Macintosh-, Windows 95- oder Windows 98-Computern haben, können Sie diesen den Zugriff auf den Java-basierten Kioskmodus gestatten, indem Sie, wie in diesem Abschnitt erläutert, in die von diesen Gruppen verwendete(n) Vorlage(n) die entsprechende Variable einfügen. Die für Vorlagen zur Verfügung stehenden Variablen werden in der folgenden Tabelle erklärt.

Variable	Durch Variable eingefügter Inhalt
$citrix_username;	Name des angemeldeten Benutzers
$citrix_portal;	Links zum Secure Access Client und zum Kioskmodus
$citrix_portal_full_client_only;	Link nur zum Secure Access Client
$citrix_portal_kiosk_client_only;	Link nur zum Kioskmodus
$citrix_activex_object_include	Fügt das ActiveX-Steuerelement ein, das die Clientportalseite startet

Pro Vorlage darf nur eine der drei Variablen enthalten sein, die mit $citrix_portal beginnen.

Bei der Auswahl einer Vorlage für eine bestimmte Gruppe müssen Sie nur wissen, ob die Gruppe Zugriff auf den Secure Access Client und den Kioskmodus oder aber nur auf einen dieser Clients haben soll. Das Access Gateway erkennt automatisch die Plattform des Benutzers (Windows, Linux, Java) und fügt in die Vorlagen, die Sie auf das Access Gateway hochladen, die entsprechenden Links ein.

So laden Sie die Portalseitenvorlagen auf den lokalen Computer herunter:

1. Klicken Sie im Administration Portal auf **Downloads**.
2. Klicken Sie unter **Download a sample portal page template that includes** mit der rechten Maustaste auf einen der Links, klicken Sie auf **Ziel speichern unter** und geben Sie im Dialogfeld, das sich daraufhin öffnet, einen Speicherort an.

So arbeiten Sie mit den Vorlagen für Windows- und Linux-Benutzer:

1. Überlegen Sie sich, wie viele benutzerdefinierte Portalseiten Sie benötigen. Portalseiten können für mehrere Gruppen verwendet werden.

Anmeldeseite	Clients, für die Links eingefügt werden
vpnAndKioskClients.html	Secure Access Client und Kioskverbindungen
vpnClientOnly.html	Nur Secure Access Client
kioskClientOnly.html	Nur Kioskverbindungen

2. Erstellen Sie Kopien der Vorlagen, die Sie verwenden möchten, und geben Sie ihnen einen Namen mit der Dateierweiterung .html.
3. Öffnen Sie die Datei im Windows-Editor oder einem HTML-Editor.
4. So ersetzen Sie das Citrix Logo:
   A. Suchen Sie in der Vorlage die folgende Zeile:

   B. Setzen Sie für **citrix-logo.gif** den Namen Ihrer Bilddatei ein. Wenn Ihre Bilddatei logo.gif heißt, muss die Zeile demnach wie folgt lauten:

   Unterstützt werden nur Bilddateien im GIF- oder JPG-Format. Lassen Sie die anderen Zeichen in der Zeile unverändert.
5. Speichern Sie die Datei.

Verwenden des ActiveX-Steuerelements

Wenn Sie die Clientanmeldeseite mit dem ActiveX-Steuerelement starten möchten, fügen Sie in die Anmeldeseitenvorlage den folgenden Code ein.

```
<html>
<head>
<title>Hallo $citrix_username;</title>
$citrix_activex_object_include;
</head>
<body>
<img src=”citrix-logo.gif”>
<br/><br/>
<b>Hallo $citrix_username;,</b>
<br/><br/>
$citrix_portal;
</body>
</html>
```

Installieren benutzerdefinierter Portalseitendateien

Benutzerdefinierte Portalseiten und die Bilddateien, auf die in den Vorlagen verwiesen wird, müssen auf dem Access Gateway installiert werden.

So wählen Sie eine Portalseite aus:

1. Klicken Sie auf der Registerkarte **Portal Page Configuration** auf die Registerkarte **Portal Pages**. Klicken Sie auf **Add File**.
2. Geben Sie im Feld **File title** den Titel der Datei ein, die Sie hinzufügen.

   Mithilfe von Dateititeln können Sie die Portalseite leicht mit einer Gruppe verknüpfen. Es kann z. B. vorkommen, dass Sie eine Hauptportalseite haben, die von vielen Gruppen verwendet wird, und eine separate Portalseite, die nur Gästen angezeigt wird. In diesem Fall können Sie die Dateien „Hauptanmeldung“ und „Gastanmeldung“ nennen. Wenn Sie mehrere Portalseiten haben, die bestimmten Benutzergruppen entsprechen, bieten sich Namen wie „Adminanmeldung“, „Studentenanmeldung“ oder „IT-Anmeldung“ an.
3. Wählen Sie unter **File Type** ein Dateiformat aus.

   Portalseiten müssen HTML-Dateien sein. Bilder, auf die auf einer HTML-Seite verwiesen wird, müssen entweder im GIF- oder im JPG-Format vorliegen.
4. Klicken Sie auf **Upload File**.
5. Gehen Sie zur Datei und klicken Sie auf **Öffnen**.

   Die Datei wird auf das Access Gateway geladen.

So entfernen Sie eine Portaldatei vom Access Gateway:

Wählen Sie in der Liste auf der Registerkarte **Portal Page Configuration** die Seiten-ID der Datei aus und klicken Sie auf **Remove Selected File**.

Einfügen von Links zu Clients auf Ihrer Website

Sie können auf Ihrer Website Links zum Secure Access Client und zum Kioskmodus einfügen, über die die Benutzer direkt auf diese Clients zugreifen können. Die Links starten die Clients für Windows oder leiten den Benutzer zu einer Seite weiter, auf der das Herunterladen und Installieren des Secure Access Client für Linux erläutert wird.

So fügen Sie auf Ihrer Website Links zum Secure Access Client und zum Kioskmodus ein:

1. Fügen Sie dem HEAD-Tag der Webseite, auf der die Links erscheinen sollen, den folgenden Code hinzu:

```
<object id="Net6Launch" type="application/x-oleobject"
classid="CLSID:7E0FDFBB-87D4-43a1-9AD4-41F0EA8AFF7B"
codebase="net6helper.cab#version=2,1,0,6">
</object>
```

2. Fügen Sie der Webseite wie folgt Links hinzu:

Client	Linkziel
Secure Access Client (Windows/Java)	https://*IP-Adresse*/CitrixSAClient.exe
Kioskmodus (Windows/ Java)	https://*IP-Adresse*/CitrixSAKiosk.exe
Secure Access Client (Linux)	https://*IP-Adresse*/full_linux_instructions.html, wobei *IP-Adresse* die Adresse des Access Gateways ist. Diese Seite enthält einen Link zur Linux-Installationsprogrammdatei.

Auswählen einer Portalseite für eine Gruppe

Standardmäßig melden sich alle Benutzer am Access Gateway über den Secure Access Client an. Der Zugriff auf den Secure Access Client kann über die Standardportalseite erfolgen oder die Benutzer laden den Client herunter und installieren ihn lokal auf ihrem Computer. Sie können benutzerdefinierte Portalseiten auf das Access Gateway laden (Informationen hierzu finden Sie unter „Installieren benutzerdefinierter Portalseitendateien“ auf Seite 188) und dann für jede Gruppe eine Portalseite auswählen. Auf diese Weise können Sie steuern, welche Access Gateway-Clients für die jeweiligen Gruppen verfügbar sind.

Hinweis: Das Deaktivieren der Anmeldeseitenauthentifizierung auf der Registerkarte **Global Cluster Policies** überschreibt die Anmeldeseiteneinstellung für alle Gruppen. Weitere Informationen hierzu finden Sie unter „Aktivieren der Anmeldeseitenauthentifizierung“ auf Seite 183.

So legen Sie eine Portalseite für eine Gruppe fest:

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** unter **User Groups** auf eine Gruppe und klicken Sie dann auf **Properties**.
2. Klicken Sie auf der Registerkarte **Gateway Portal** unter **Portal configuration** auf **Use custom portal page** und wählen Sie dann die Seite aus. Klicken Sie auf **OK**.

Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen

Sie können festlegen, dass den Benutzern eine Webseite angezeigt wird, auf der diese wählen können, ob sie sich über den Secure Access Client, das Webinterface oder den Kioskmodus anmelden möchten. Diese Portalseite kann im Gegensatz zur Standardportalseite nicht konfiguriert werden. Dem Benutzer werden drei Symbole angezeigt und er kann dann wählen, mit welchem der folgenden Verfahren er sich am Access Gateway anmelden möchte: LOESCHEN

Secure Access Client: Dieses Symbol startet den Secure Access Client. Nach der Anmeldung des Clients wird das Webinterface angezeigt.

Webinterface-Anmeldung: Mit diesem Symbol wird der Benutzer zum Webinterface weitergeleitet.

Kioskverbindung: Mit diesem Symbol kann sich der Benutzer im Kioskmodus anmelden.

Diese Portalseite wird nur dann angezeigt, wenn auf der Registerkarte **Gateway Portal** die Optionen **Redirect to Web Interface** und **Use the multiple logon option page** aktiviert sind.

So konfigurieren Sie mehrere Anmeldeoptionen:

1. Klicken Sie mit der rechten Maustaste im linken Bereich der Registerkarte **Access Policy Manager** auf eine Gruppe und klicken Sie dann auf **Properties**.
2. Wählen Sie auf der Registerkarte **Gateway Portal** die Option **Redirect to Web Interface**.
3. Geben Sie im Feld **Path** den Pfad des Servers ein, auf dem das Webinterface gehostet wird. Die Standardeinstellung ist Citrix/MetaFrame/auth/Login.aspx.
4. Geben Sie im Feld **Web server** die IP-Adresse oder den FQDN des Servers ein, auf dem das Webinterface gehostet wird.
5. Klicken Sie auf **Use a secure connection**, um die Verbindung zu sichern.
6. Wenn sich die Benutzer über den Secure Access Client anmelden können sollen, aktivieren Sie die Option **Use the multiple logon option page**. Klicken Sie auf **OK**.

Hinweis: Das Webinterface muss Verbindungen vom Access Gateway unterstützen, um diese Konfiguration abschließen zu können. Weitere Informationen zum Konfigurieren des Webinterface finden Sie unter „Bereitstellen von Zugriff auf veröffentlichte Anwendungen“ auf Seite 193.

Anmelden mit Zweimethodenauthentifizierung

Wenn das Access Gateway so konfiguriert ist, dass Benutzer sich mit zwei verschiedenen Authentifizierungsverfahren, wie LDAP und RSA SecurID, anmelden müssen, werden die Benutzer automatisch zur entsprechenden Webseite oder zum Secure Access Client-Dialogfeld weitergeleitet, wo sie ihren Benutzernamen und ihre Kennwörter eingeben können. Weitere Informationen zur Zweimethodenauthentifizierung finden Sie unter „Konfigurieren von Zweimethodenauthentifizierung“ auf Seite 110.

Wenn Sie möchten, dass die Kennwort-Label den Authentifizierungstyp beschreiben, mit dem sich Benutzer anmelden, können Sie diese Label ändern. Weitere Informationen hierzu finden Sie unter „Ändern der Beschriftung von Kennwortfeldern“ auf Seite 111.

Anmelden, wenn Vorauthentifizierungsrichtlinien konfiguriert sind

Wenn auf dem Access Gateway eine Richtlinie zur Prüfung vor der Authentifizierung konfiguriert wurde und der Benutzer eine Webadresse eingibt, um eine Verbindung herzustellen, wird der Computer des Benutzers auf die Einhaltung der in der Richtlinie enthaltenen Kriterien geprüft, während dem Benutzer eine Webseite ohne die Möglichkeit der Eingabe von Anmeldeinformationen angezeigt wird. Falls der Clientcomputer die Richtlinienüberprüfung vor der Authentifizierung besteht, werden die Benutzer mit der Anmeldeseite verbunden, von wo aus sie sich mit ihren Anmeldeinformationen am Access Gateway anmelden können. Sollte die Überprüfung des Computers ein negatives Ergebnis erbringen, erhält der Benutzer eine Fehlermeldung, in der er aufgefordert wird, sich mit dem Systemadministrator in Verbindung zu setzen.

Weitere Informationen hierzu finden Sie unter „Konfigurieren von Richtlinien zur Überprüfung vor der Authentifizierung“ auf Seite 137.

Bereitstellen von Zugriff auf veröffentlichte Anwendungen

Eine Serverfarm besteht aus mindestens einem Computer, auf dem Citrix Presentation Server ausgeführt wird. Wenn Ihr Unternehmensnetzwerk eine Serverfarm enthält, können Sie das Access Gateway implementieren und so sicheren Internetzugang auf veröffentlichte Ressourcen bereitstellen.

Bei solchen Implementierungen arbeitet das Access Gateway mit dem Webinterface und der Secure Ticket Authority (STA) zusammen, um die Authentifizierung, Autorisierung sowie Umleitung auf veröffentlichte Ressourcen auf einem Computer bereitzustellen, auf dem Citrix Presentation Server ausgeführt wird.

Access Gateway kann mit den Webinterface-Versionen 3.0, 4.0, 4.2 und 4.5 verwendet werden.

In diesem Kapitel werden folgende Themen behandelt:

- Benutzerverbindungen zu einer Serverfarm
- Ersetzen von Secure Gateway
- Konfigurieren des Webinterface
- Konfigurieren des Webinterface für die Authentifizierung
- Konfigurieren der Secure Ticket Authority
- Konfigurieren der ICA-Zugriffssteuerung
- Verwenden des Webinterface als Anmeldeseite
- Konfigurieren von Single Sign-On beim Webinterface
- Aktivieren der Sitzungszuverlässigkeit

Benutzerverbindungen zu einer Serverfarm

Benutzer können sich über Citrix Presentation Server Clients mit dem Unternehmensnetzwerk verbinden, um Zugriff auf veröffentlichte Anwendungen in der Serverfarm zu erhalten. Clientverbindungen funktionieren wie in einer Secure Gateway-Bereitstellung. Der einzige Unterschied ist, dass Secure Gateway aus der DMZ entfernt und durch das Access Gateway ersetzt wird. Weitere Informationen zum Ersetzen von Secure Gateway finden Sie unter „Ersetzen von Secure Gateway“ auf Seite 197.

Citrix Presentation Server Clients können von verschiedenen Geräten aus eine Verbindung herstellen, z. B. von Computern und Handheld-PDAs, während der Secure Access Client nur von einem Windows-Computer aus Verbindungen herstellen kann.

Wenn Citrix Presentation Server Clients die einzigen Clients sind, die eine Verbindung zu einer Serverfarm herstellen, kann kein Failover für das Access Gateway verwendet werden. Nur der Secure Access Client unterstützt Failover.

Citrix empfiehlt zwei Möglichkeiten der Verbindungen zum Unternehmensnetzwerk:

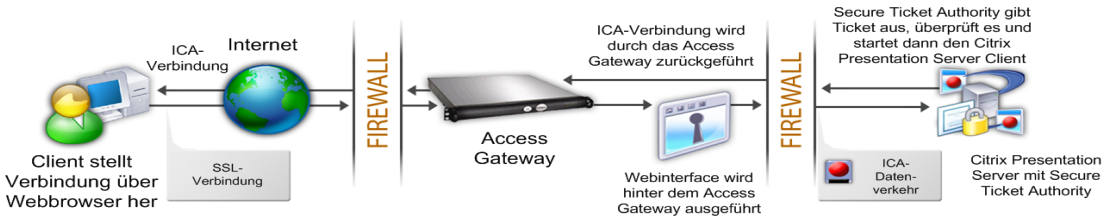
- Direkte Verbindungen zu veröffentlichten Anwendungen über Citrix Presentation Server Clients
- Direkte Verbindungen zu veröffentlichten Anwendungen über Citrix Presentation Server Clients und Verbindungen zu anderen Unternehmensressourcen über den Secure Access Client

---

Hinweis: Wenn Sie das Access Gateway in einer Double-Hop-DMZ bereitgestellt haben, kann der Secure Access Client nicht verwendet werden. Weitere Informationen hierzu finden Sie unter „Bereitstellen des Access Gateways in einer Double-Hop-DMZ“ auf Seite 223.

Verbindungen mit Citrix Presentation Server-Clients. Bei diesem Szenario öffnet der Benutzer einen Webbrowser und gibt den vollqualifizierten Domänennamen oder die IP-Adresse des Access Gateways ein. Wenn die Portalseitenauthentifizierung aktiviert ist, meldet sich der Benutzer an und wird authentifiziert. Sobald die Authentifizierung erfolgt ist, wird das Webinterface geöffnet, das hinter dem Access Gateway ausgeführt wird. Das Webinterface verhandelt mit der STA (Secure Ticket Authority) und zeigt dann eine Liste der veröffentlichten Anwendungen an. Wenn der Client auf eine veröffentlichte Anwendung klickt, verwendet er die im Webinterface konfigurierten STA-Informationen, und wenn das Ticket an den Client zurückgesendet wird, wird die ICA-Verbindung über den Citrix Presentation Server Client hergestellt. In diesem Szenario wird der Secure Access Client nicht verwendet. Zur Herstellung einer Verbindung über das Access Gateway präsentiert der Client dem Access Gateway das Ticket. Anschließend überprüft das Access Gateway das Ticket anhand seiner Serverliste.

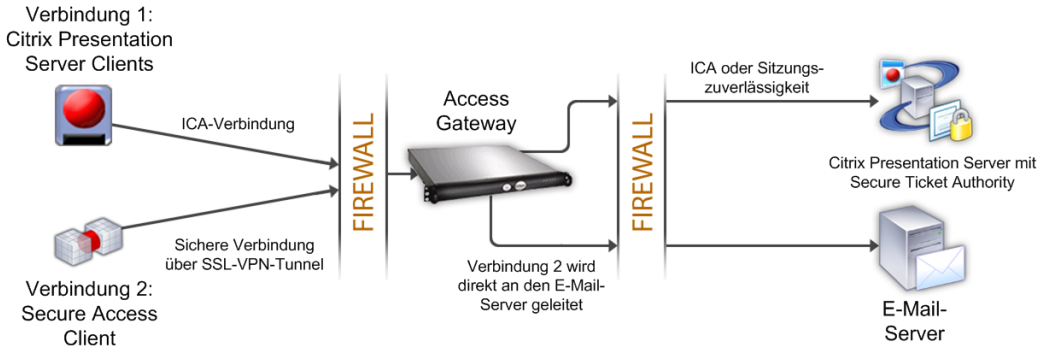
Wenn eine ICA-Verbindung über Citrix Presentation Server Clients hergestellt wurde, wird die Authentifizierung des Clientzertifikats nicht unterstützt.


ICA-Verbindung
Internet
FIREWALL
ICA-Verbindung wird durch das Access Gateway zurückgeführt
Secure Ticket Authority gibt Ticket aus, überprüft es und startet dann den Citrix Presentation Server Client
Client stellt Verbindung über Webbrowser her
SSL-Verbindung
Access Gateway
Webinterface wird hinter dem Access Gateway ausgeführt
FIREWALL
ICA-Daten-verkehr
Citrix Presentation Server mit Secure Ticket Authority

Herstellen der Verbindung von Citrix Presentation Server Clients mit einer Serverfarm

Direkte Verbindungen mit Citrix Presentation Server Client und Secure Access Client. In diesem Szenario kann der Benutzer über zwei separate Verbindungen gleichzeitig eine Verbindung zum Unternehmensnetzwerk herstellen. Die erste Verbindung verwendet einen Presentation Server Client, um die Verbindung mit den oben aufgeführten Schritten herzustellen.

Falls Benutzer auf andere Ressourcen im Unternehmensnetzwerk zugreifen müssen, können Sie sich auch über den Secure Access Client anmelden. Beispiel: Ein Benutzer möchte im Unternehmensnetzwerk eine Verbindung mit einem Microsoft Exchange Server herstellen. Er startet Microsoft Outlook auf seinem Computer. Es wird eine sichere Verbindung mit dem Secure Access Client hergestellt, der wiederum eine Verbindung zum Access Gateway herstellt. Der SSL-VPN-Tunnel zum Exchange-Server wird hergestellt, sodass der Benutzer seine E-Mails abrufen kann.



Gleichzeitige Verbindung mit Citrix Presentation Server Client und Secure Access Client

Wenn das Webinterface für die Authentifizierung oder den Zugriff auf Ressourcen in der Serverfarm konfiguriert ist, kann es im sicheren Netzwerk implementiert werden. Falls das Webinterface hinter dem Access Gateway ausgeführt wird, empfiehlt Citrix, die Authentifizierung auf dem Access Gateway zu konfigurieren.

Wichtig: Wenn sich das Webinterface im sicheren Netzwerk befindet, muss die Anmeldeseitenauthentifizierung auf dem Access Gateway aktiviert sein. Wenn die Anmeldeseitenauthentifizierung deaktiviert ist, werden nicht authentifizierte HTTP-Anforderungen direkt an den Server gesendet, auf dem das Webinterface ausgeführt wird. Die Deaktivierung der Anmeldeseitenauthentifizierung wird nur empfohlen, wenn sich das Webinterface in der DMZ befindet und Benutzer eine direkte Verbindung zum Webinterface herstellen.

Weitere Informationen zum Bereitstellen des Webinterface mit dem Access Gateway finden Sie unter „Konfigurieren des Webinterface“ auf Seite 204.

Ersetzen von Secure Gateway

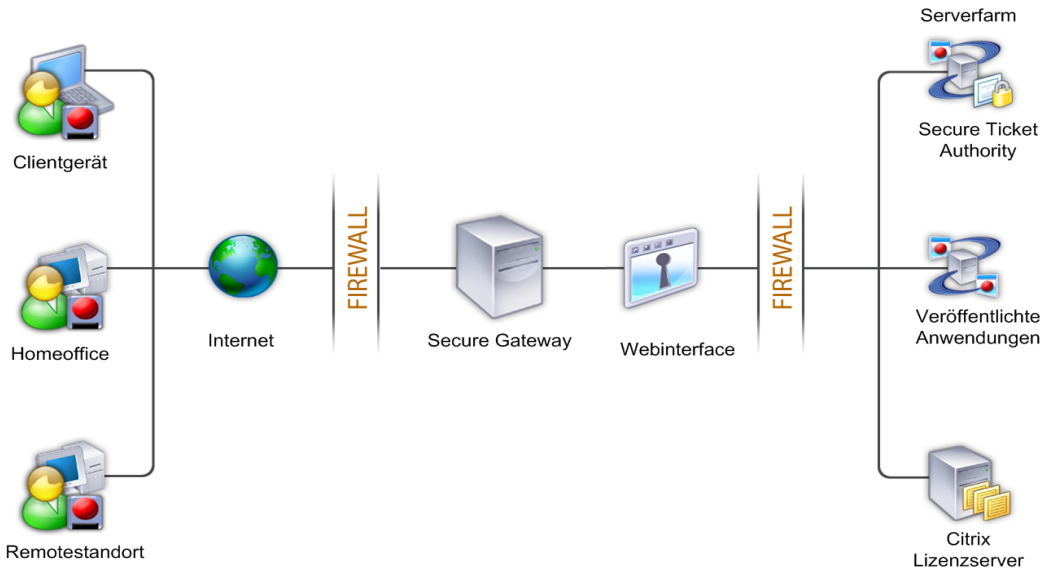
Wenn Sie derzeit Secure Gateway verwenden, um Remotezugriff auf Server zuzulassen, auf denen Citrix Presentation Server ausgeführt wird, können Sie Secure Gateway durch das Access Gateway ersetzen.

Einer der Vorteile, die Secure Gateway-Software durch das hardwarebasierte Access Gateway-Gerät zu ersetzen, ist unter anderem die Unterstützung zusätzlicher Anwendungen. Da Secure Gateway nur Presentation Server-Verkehr unterstützt, setzen Organisationen, die Secure Gateway verwenden, möglicherweise noch eine zusätzliche Lösung für den Remotezugriff auf andere Arten von Unternehmensressourcen ein, wodurch zusätzliche Ausgaben und Gemeinkosten entstehen. Das Access Gateway kann alle Ansprüche Ihrer Organisation für den Remotezugriff erfüllen, indem es sowohl den Verkehr zu auf Presentation Server gehosteten Anwendungen als auch den Zugriff auf Unternehmensressourcen wie E-Mail, internen Webanwendungen sowie Netzfreigaben sichert.

Sowohl das Access Gateway als auch Secure Gateway unterstützen Verbindungen zwischen Presentation Server Clients und veröffentlichten Anwendungen in Single- und Double-Hop-DMZ-Bereitstellungen.

Hinweis: Wenn das Access Gateway in einer Double-Hop-DMZ bereitgestellt wird, werden nur Verbindungen zwischen Presentation Server Clients und veröffentlichten Anwendungen sowie HTTP-Verbindungen zu Access Gateway Advanced Edition unterstützt. In diesem Szenario unterstützt das Access Gateway keine Verbindungen zu zusätzlichen Unternehmensressourcen über den Secure Access Client. Weitere Informationen zur Bereitstellung des Access Gateways in einer Double-Hop-DMZ finden Sie unter „Bereitstellen des Access Gateways in einer Double-Hop-DMZ“ auf Seite 223 und im *Administratorhandbuch für Citrix Access Gateway Advanced Edition*.

Die folgende Abbildung zeigen eine Standardimplementierung von Secure Gateway und eine Access Gateway-Bereitstellung:



Secure Gateway-Bereitstellung mit Webinterface in der DMZ und Verbindung zu Computern, auf denen Citrix Presentation Server ausgeführt wird

In dieser Bereitstellung wird Secure Gateway auf einem Windows-Server in der DMZ ausgeführt. Das Webinterface wird auch in der DMZ bereitgestellt. Citrix Presentation Server wird im sicheren Netzwerk ausgeführt. Die Secure Ticket Authority wird auf einem Computer installiert, auf dem Presentation Server ausgeführt wird, und veröffentlichte Anwendungen werden auf einem zweiten Server in der Farm installiert.

Die folgende Abbildung zeigt das Access Gateway in der DMZ und das Webinterface im sicheren Netzwerk.

Eine Access Gateway-Bereitstellung, bei der sich das Webinterface im sicheren Netzwerk befindet. Die Computer im sicheren Netzwerk führen Citrix Presentation Server mit der Secure Ticket Authority und dem Citrix Lizenzserver aus.

Wenn Secure Gateway aus der DMZ entfernt und durch das Access Gateway ersetzt wird, haben Sie die Möglichkeit, das Webinterface in das sichere Netzwerk zu verschieben. Das Access Gateway authentifiziert und autorisiert Benutzer und stellt dann eine Verbindung zum Webinterface her. Dadurch wird die Sicherheit erhöht, da sich in der DMZ zwei Windows-Server weniger befinden.

Wichtig: Wenn sich das Webinterface im sicheren Netzwerk befindet, müssen Authentifizierung und Autorisierung auf dem Access Gateway konfiguriert werden. Weitere Informationen hierzu finden Sie unter „Konfigurieren der Authentifizierung und Autorisierung“ auf Seite 77.

Das Ersetzen von Secure Gateway durch das Access Gateway hat unter anderem folgende Vorteile:

- Ersetzen eines Windows-basierten Servers in der DMZ durch ein zusätzlich abgesichertes Gerät
- Hinzufügen von SSL-VPN-Funktionalität bei unverändertem Zugriff auf veröffentlichte Anwendungen
- Herstellen von Verbindungen von verschiedenen Clientgeräten zu veröffentlichten Anwendungen im sicheren Netzwerk mit Citrix Presentation Server Clients

Vorbereiten der Migration auf das Access Gateway

Vor der Migration von Secure Gateway auf das Access Gateway müssen folgende Punkte berücksichtigt werden:

- Stellen Sie sicher, dass Clientgeräte die Systemanforderungen erfüllen. Weitere Informationen hierzu finden Sie im *Client für Windows-Administratorhandbuch* sowie unter „Systemvoraussetzungen“ auf Seite 140.
- Stellen Sie sicher, dass Port 443 (der Standardsicherheitsport) in der Firewall zwischen dem Internet und dem Access Gateway geöffnet ist. Diese Anforderung entspricht einer Secure Gateway-Bereitstellung.

  Access Gateway Version 4.5 verfügt über eine Funktion zur Portumleitung. Sie können sämtlichen Netzwerkverkehr durch Port 80 verhindern oder den Verkehr für diesen Port an einen sicheren Port (typischerweise an Port 443) umleiten. Weitere Informationen hierzu finden Sie unter „Umleiten von Verbindungen auf Port 80 an einen sicheren Port“ auf Seite 47.
- Installieren Sie das Access Gateway gemäß den Anweisungen unter „Erstmalige Installation des Access Gateways“ auf Seite 39.
- Erwerben und installieren Sie die entsprechenden Zertifikate auf dem Access Gateway. Dazu gehören folgende Zertifikate:
  - Serverzertifikat für das Access Gateway. Der vollqualifizierte Domänenname auf dem Zertifikat muss mit dem vollqualifizierten Domänennamen des Access Gateways übereinstimmen.
  - Stammzertifikate für das Access Gateway, für die Secure Ticket Authority sowie für Clientgeräte.

  Weitere Informationen zum Installieren von Zertifikaten auf dem Access Gateway finden Sie unter „Erstellen und Installieren von Zertifikaten“ auf Seite 55. Nähere Erläuterungen zur Zertifikattechnologie finden Sie unter „Sichern von Verbindungen mit digitalen Zertifikaten“ auf Seite 291.
- Konfigurieren Sie die Netzwerke, zu denen Benutzer eine Verbindung über das Access Gateway herstellen können. Weitere Informationen zur Konfiguration des Netzwerkzugriffs für Benutzer finden Sie unter „Konfigurieren von Netzwerkzugriff und Gruppenressourcen“ auf Seite 113.

Weitere Informationen zur Installation des Access Gateways finden Sie im Handbuch *Installationsübersicht für Citrix Access Gateway Standard Edition* und in der *Citrix Access Gateway Standard Edition Pre-Installation Checklist*.

Migrieren von Secure Gateway auf das Access Gateway

Es gibt zwei Optionen für die Migration von Secure Gateway zum Access Gateway:

- In-Place-Migration: Hierbei werden das Zertifikat und der vollqualifizierte Domänenname vom Secure Gateway auf das Access Gateway übertragen.
- Parallel-Migration: Hier werden ein neues Zertifikat und ein vollqualifizierter Domänenname für das Access Gateway abgerufen.

Jede Option ist zulässig; bei der In-Place-Migration kann es jedoch im Gegensatz zu einer neuen Installation zu einer vorübergehenden Unterbrechung des Zugriffs auf Unternehmensressourcen kommen.

Nach Abschluss der Migration können sich Benutzer ohne jede weitere Konfiguration an ihrem Gerät mit ihren üblichen Benutzeranmeldeinformationen anmelden, was den Support für den Benutzer auf ein Minimum reduziert.

Durchführen einer In-Place-Migration

Wenn Sie sich für die In-Place-Migration von Secure Gateway auf das Access Gateway entschieden haben, exportieren Sie das Secure Gateway-Zertifikat und laden Sie es auf das Access Gateway hoch.

Das Zertifikat muss im PEM-Format vorliegen, bevor es auf dem Access Gateway installiert werden kann. Weitere Informationen zum Konvertieren eines Zertifikats in ein PEM-Format mit Win32 OpenSSL finden Sie unter „Verwenden von Windows-Zertifikaten“ auf Seite 301. Falls Sie mit dem Konvertieren von Zertifikaten nicht vertraut sind, empfiehlt Citrix die Neuinstallation des Access Gateways mit einem neuen Zertifikat.

Wichtig: Wenn Sie das Zertifikat von Secure Gateway auf das Access Gateway übertragen, muss der vollqualifizierte Domänenname des Access Gateways mit dem des Secure Gateways übereinstimmen.

Mit dieser Option ist keine stufenweise Vorgehensweise möglich, da sich nicht zwei identische vollqualifizierte Domänennamen im selben Netzwerk befinden dürfen.

Mit Ausnahme folgender Elemente entspricht eine In-Place-Migration einer Neuinstallation:

- Auf dem Access Gateway wird ein PEM-formatiertes Secure Gateway-Zertifikat verwendet.
- Der vollqualifizierte Domänenname auf dem Access Gateway wird so verändert, dass er mit dem von Secure Gateway identisch ist.

Falls die Anmeldeseite des Access Gateways so konfiguriert ist, dass sie genauso aussieht wie die von Secure Gateway, bemerken Benutzer eventuell nicht, dass sie sich über dieses Gerät anmelden. Auch wenn die In-Place-Migration den geringsten Aufwand an Support erfordert (es ist nicht erforderlich, Benutzer über eine neue Webadresse zu informieren), hat es direkte Auswirkungen auf alle Benutzer, wenn bei der Konfiguration des Access Gateways Fehler gemacht wurden, die trotz einer ausführlichen Testphase nicht erkannt wurden.

Durchführen einer Parallel-Migration

Als beste Vorgehensweise empfiehlt Citrix, dass Secure Gateway solange parallel mit dem Access Gateway ausgeführt wird, bis alle Benutzer ordnungsgemäß auf das Gerät migriert worden sind. Für eine Parallel-Migration ist folgendes erforderlich:

- Ein neuer vollqualifizierter Domänenname und ein neues Zertifikat für das Access Gateway. Weitere Informationen zum Erwerb eines Zertifikats finden Sie unter „Erstellen und Installieren von Zertifikaten“ auf Seite 55
- Geben Sie den Benutzern die neue für den Zugriff auf Unternehmensressourcen erforderliche Webadresse sowie das Datum, an dem mit der Verwendung des Access Gateways begonnen wird.

Durch eine Parallel-Migration haben Sie mehr Kontrolle über die Konfiguration und können im Gegensatz zur gleichzeitigen Übertragung sämtlicher Benutzer bei einer In-Place-Migration stufenweise vorgehen. Benutzer können in Gruppen auf das Access Gateway migriert werden, wodurch eine Ausfallzeit der Verbindungen vermieden wird.

Die Durchführung einer Parallel-Migration entspricht einer Neuinstallation des Access Gateways. Bei dieser Möglichkeit wird das Secure Gateway solange parallel zum Access Gateway ausgeführt, bis sämtliche Benutzer erfolgreich in die neue Umgebung migriert wurden. Bei dieser Variante müssen Sie ein neues Serverzertifikat erwerben oder generieren. Dadurch wird jedoch sichergestellt, dass es für die Benutzer zu keinen Zugriffsunterbrechungen auf Unternehmensressourcen kommt.

Führen Sie für eine Parallel-Migration auf das Access Gateway folgende Schritte aus:

Schritt 1: Installieren Sie das Access Gateway wie unter „Erstmalige Installation des Access Gateways“ auf Seite 39 beschrieben. In diesem Schritt werden die grundlegenden TCP/IP-Einstellungen für das Access Gateway konfiguriert.

Schritt 2: Konfigurieren Sie die Einstellungen für die Secure Ticket Authority auf dem Access Gateway mit dem Administration Tool, um eine Verbindung zu Ressourcen auf Computern, auf denen Citrix Presentation Server ausgeführt wird, herzustellen. Weitere Informationen hierzu finden Sie unter „Konfigurieren der Secure Ticket Authority“ auf Seite 212. Wenn die Secure Ticket Authority konfiguriert ist, wird sie im Administration Tool auf der Registerkarte **Authentication > Security Ticket Authority** aufgeführt.

Hinweis: Sie können der Liste mehrere Server hinzufügen, auf denen die Secure Ticket Authority ausgeführt wird. Die Liste der Server muss den Servern entsprechen, die für das Webinterface konfiguriert sind.

Schritt 3: Installieren Sie zur Sicherung der Clientverbindungen ein Serverzertifikat auf dem Access Gateway.

Konfigurieren Sie zum Verwenden auflösbarer Namen für die Secure Ticket Authority und das Webinterface Ihre DNS-Server. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Namensdienstanbietern“ auf Seite 62.

Schritt 4: Konfigurieren Sie die Einstellungen für den Benutzerzugriff im Webinterface. Weitere Informationen hierzu finden Sie unter „Einrichten und Testen des Webinterface“ auf Seite 209.

Schritt 5: Entfernen Sie das Webinterface aus der DMZ und platzieren Sie es im sicheren Netzwerk.

Der Server, auf dem Secure Gateway ausgeführt wird, kann außer Betrieb genommen und für einen anderen Zweck verwendet werden.

So testen Sie Benutzerverbindungen mit dem Access Gateway:

1. Klicken Sie auf der Registerkarte **Access Policy Manager** mit der rechten Maustaste auf den Ordner **Local Users** und klicken Sie auf **New User**.
2. Geben Sie im Dialogfeld **User Name** in das Feld **User Name** einen Benutzernamen ein und in das Feld **Password** und **Verify Password** das entsprechende Kennwort und klicken Sie auf **OK**.
3. Klicken Sie mit der rechten Maustaste auf die Gruppe **Default** und klicken Sie auf **Properties**.

4. Klicken Sie auf der Registerkarte **Gateway Portal** auf **Redirect to Web Interface**, geben Sie den Standardpfad /Citrix/MetaFrame/auth/Login.aspx ein und klicken Sie auf **OK**.
5. Geben Sie im Webbrowser als Adresse des Access Gateways den vollqualifizierten Domänennamen ein.

   Das Format ist folgendermaßen: https://*vollqualifizierter Domänenname*.
6. Geben Sie die Anmeldeinformationen ein.
7. Falls auf der Registerkarte **Global Cluster Policies** die Option **Enable logon page authentication** aktiviert ist, melden Sie sich an. Darauf wird die Webinterface-Seite angezeigt.

Wenn Single Sign-On beim Webinterface eingestellt ist, werden Benutzer automatisch angemeldet und haben Zugriff auf veröffentlichte Anwendungen. Andernfalls melden sich Benutzer am Webinterface an und haben dann Zugriff auf ihre veröffentlichten Anwendungen.

Informationen dazu, wie Sie Verbindungen zum Webinterface testen können, finden Sie unter „So überprüfen Sie die Webinterface-Einstellungen:“ auf Seite 212.

Überwachen des Access Gateways nach der Installation

Da Benutzer von Secure Gateway zum Access Gateway verschoben werden, muss die Leistung insbesondere in den ersten Tagen nach der Implementierung überwacht werden, damit gewährleistet ist, dass es bei den Benutzern zu keinen Problemen kommt. Die Überwachung des Access Gateways erfolgt über den Administration Desktop, der den Zugriff auf eine Vielzahl von Standardtools für die Netzwerküberwachung bietet. Der Administration Desktop bietet auch Zugriff auf den Real-time Monitor, mit dem eine Liste der aktuellen Benutzer angezeigt werden kann. Weitere Informationen zum Administration Desktop und zu den Netzwerktools finden Sie unter „Überwachen des Access Gateways“ auf Seite 283.

Konfigurieren des Webinterface

Das Webinterface kann auf einem Server in der DMZ oder im sicheren Netzwerk ausgeführt werden. Bei Herstellung einer Clientverbindung wird die Authentifizierung vom Webinterface durchgeführt.

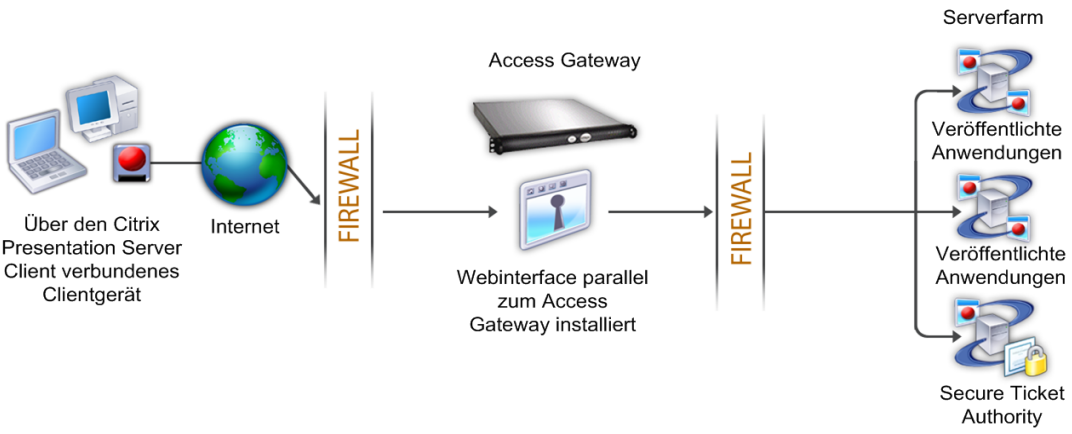
Weitere Informationen zum Konfigurieren der Authentifizierung auf dem Access Gateway finden Sie unter „Voraussetzungen zum Konfigurieren der Authentifizierung auf dem Access Gateway“ auf Seite 78.

Bereitstellen des Webinterface parallel zum Access Gateway in der DMZ

In dieser Bereitstellung befinden sich Webinterface und Access Gateway beide in der DMZ. Benutzer stellen über einen Webbrowser direkt eine Verbindung zum Webinterface her. Benutzer haben sofort nach der Anmeldung am Webinterface Zugriff auf veröffentlichte Anwendungen in der Serverfarm. Sobald ein Benutzer eine Anwendung startet, sendet das Webinterface eine ICA-Datei mit Anweisungen zum Routen des ICA-Verkehrs durch das Access Gateway, als ob es ein Server wäre, auf dem Secure Gateway ausgeführt wird. Die vom Webinterface gelieferte ICA-Datei enthält ein von der Secure Ticket Authority ausgestelltes Sitzungsticket.

Das Ticket wird bereitgestellt, sobald der Presentation Server Client eine Verbindung zum Access Gateway herstellt. Das Access Gateway ruft die Secure Ticket Authority auf, um das Sitzungsticket zu validieren. Wenn das Ticket noch gültig ist, wird der ICA-Verkehr des Benutzers an den Server in der Serverfarm weitergeleitet.

Wenn das Webinterface parallel zum Access Gateway in der DMZ ausgeführt wird, muss keine Authentifizierung auf dem Access Gateway konfiguriert werden.



Das Webinterface ist parallel zum Access Gateway installiert. Clientverbindungen werden zur Authentifizierung zuerst zum Webinterface gesendet. Nach der Authentifizierung werden die Verbindungen durch das Access Gateway weitergeleitet.

Konfigurieren von Smartcardzugriff mit dem Webinterface

Wenn Benutzer sich mit Citrix Presentation Server Clients direkt beim Webinterface anmelden und Smartcardauthentifizierung verwenden, muss sich das Webinterface parallel zum Access Gateway in der DMZ befinden. Außerdem muss der Server, auf dem das Webinterface ausgeführt wird, ein Mitglied der Domäne sein.

Wenn sich Benutzer mit dem Secure Access Client anmelden, erfolgt die erste Authentifizierung durch das Access Gateway. Wenn ein VPN-Tunnel eingerichtet ist, kann der Benutzer sich mit der Smartcard am Webinterface anmelden. In diesem Szenario kann das Webinterface hinter dem Access Gateway oder im sicheren Netzwerk installiert werden.

Wenn das Webinterface für die Verwendung von Smartcardauthentifizierung konfiguriert und parallel zum Access Gateway installiert ist, beenden das Access Gateway und das Webinterface beide einen Teil der SSL-Verbindung.

Das Webinterface beendet den sicheren HTTP-Verkehr einschließlich der Benutzerauthentifizierung, der Anzeige und dem Starten veröffentlichter Anwendungen.

Das Access Gateway beendet ICA-Verbindungen, die über die sichere Verbindung durch den Tunnel geleitet werden.

Bereitstellen des Webinterface hinter dem Access Gateway in der DMZ

Damit der gesamte HTTPS- und ICA-Verkehr durch einen einzigen externen Port gesendet werden kann und nur ein einziges SSL-Zertifikat benötigt wird, kann das Access Gateway als Reverse-Webproxy für das Webinterface fungieren.

Wenn das Webinterface hinter dem Access Gateway in der DMZ implementiert ist, kann die Authentifizierung auf dem Gerät konfiguriert werden, dies ist jedoch nicht zwingend erforderlich.

Zum Implementieren des Webinterface hinter dem Access Gateway müssen Sie die Eigenschaften der Standardbenutzergruppe bzw. die Eigenschaften der Gruppe, für die der Zugriff auf das Webinterface aktiviert werden soll, bearbeiten.

So konfigurieren Sie das Webinterface auf dem Access Gateway:

1. Klicken Sie auf der Registerkarte **Access Policy Manager** mit der rechten Maustaste auf eine Benutzergruppe und klicken Sie dann auf **Properties**.
2. Wählen Sie auf der Registerkarte **Gateway Portal** die Option **Redirect to Web Interface**.
3. Geben Sie unter **Path** den Pfad /Citrix/Metaframe/auth/Login.aspx ein.

4. Geben Sie im Feld **Web server** die IP-Adresse oder den vollqualifizierten Domänennamen des Servers ein, auf dem das Webinterface ausgeführt wird. Klicken Sie auf **OK**.

Bereitstellen des Webinterface im sicheren Netzwerk

Bei dieser Bereitstellung befindet sich das Webinterface in dem vertrauenswürdigen Netzwerk. Das Access Gateway befindet sich in der DMZ. Benutzeranforderungen werden vom Access Gateway authentifiziert, bevor Sie an das Webinterface gesendet werden.

Bei einer Bereitstellung des Webinterface im sicheren Netzwerk muss die Authentifizierung auf dem Access Gateway konfiguriert werden. Benutzer melden sich am Access Gateway an, geben ihre Anmeldeinformationen ein und werden dann mit dem Webinterface verbunden.

Wichtig: Wenn sich das Webinterface im sicheren Netzwerk befindet, muss die Anmeldeseitenauthentifizierung auf dem Access Gateway aktiviert sein. Wenn die Anmeldeseitenauthentifizierung deaktiviert ist, werden nicht authentifizierte HTTP-Anforderungen direkt an den Server gesendet, auf dem das Webinterface ausgeführt wird. Die Deaktivierung der Anmeldeseitenauthentifizierung wird nur empfohlen, wenn sich das Webinterface in der DMZ befindet und Benutzer eine direkte Verbindung zum Webinterface herstellen.

So aktivieren Sie die Anmeldeseitenauthentifizierung:

Deaktivieren Sie auf der Registerkarte **Global Cluster Policies** unter **Advanced options** die Option **Enable logon page authentication**.

Konfigurieren des Webinterface für die Authentifizierung

Das Webinterface kann auf einem Server in der DMZ oder im sicheren Netzwerk ausgeführt werden. Wenn Benutzer mit Presentation Server Clients eine Verbindung herstellen, überprüft die Secure Ticket Authority die Authentifizierung, die vom Webinterface bereitgestellt wird.

Wichtig: Wenn das Webinterface im sicheren Netzwerk installiert ist, empfiehlt Citrix, dass das Access Gateway den Netzwerkverkehr authentifiziert, bevor die Anforderung an das Webinterface gesendet wird. Nicht authentifizierter Netzwerkverkehr sollte innerhalb des sicheren Netzwerks nicht an das Webinterface gesendet werden dürfen.

In diesem Fall verwendet das Access Gateway das Webinterface, um einen sicheren Zugriff auf veröffentlichte Ressourcen in einem sicheren Unternehmensnetzwerk zu ermöglichen. Folgende Schritte müssen ausgeführt werden:

- Die Benutzer geben die Webadresse des Access Gateways in das Adressfeld eines Webbrowsers ein.
- Das Access Gateway empfängt die Anfrage und leitet diese an das Webinterface weiter. Wenn sich das Webinterface hinter dem Access Gateway in der DMZ oder im sicheren Netzwerk befindet, empfiehlt Citrix die Authentifizierung der Benutzer über das Access Gateway.
- Das Webinterface antwortet durch Senden einer Anmeldeseite an den Clientbrowser.
- Der Benutzer gibt gültige Benutzeranmeldeinformationen ein, die über das Access Gateway an das Webinterface gesendet werden.
- Das Webinterface wiederum sendet die Benutzeranmeldeinformationen an den Citrix XML-Dienst, der von der Serverfarm aus verfügbar ist, und fragt die Liste der Anwendungen ab, die der Benutzer verwenden darf.
- Im Webinterface wird daraufhin die Liste der veröffentlichten Ressourcen angezeigt, auf die der Benutzer zugreifen darf.
- Wenn der Benutzer auf den Link zu einer veröffentlichten Anwendung klickt, sendet das Webinterface die IP-Adresse und den Port für den angeforderten Computer, auf dem Presentation Server ausgeführt wird, an die Secure Ticket Authority und fordert ein Sitzungsticket für den Benutzer an. Die Secure Ticket Authority speichert die IP-Adresse und stellt das angeforderte Ticket für das Webinterface aus.
- Das Webinterface generiert eine ICA-Datei mit dem von der Secure Ticket Authority ausgestellten Ticket und sendet diese Datei an den Clientbrowser.

Wichtig: Die vom Webinterface generierte ICA-Datei enthält den vollqualifizierten Domänennamen oder die IP-Adresse des Access Gateways. Der Presentation Server Client erfährt zu keinem Zeitpunkt die Adresse der Server, auf denen Presentation Server ausgeführt wird.

- Der Clientwebbrowser verwendet die ICA-Datei zum Starten des Presentation Server Clients. Der Client stellt mit dem vollqualifizierten Domänennamen aus der ICA-Datei eine Verbindung zum Access Gateway her. Es kommt zum ersten SSL/TLS-Handshake, um die Identität des Access Gateways zu ermitteln.

- Das Access Gateway erhält vom Client das Sitzungsticket und kontaktiert zum Zweck der Ticketvalidierung die STA.
- Wenn das Ticket gültig ist, gibt die STA die IP-Adresse des Computers zurück, auf dem Presentation Server ausgeführt wird und auf dem sich die angeforderte Anwendung befindet. Wenn das Sitzungsticket ungültig oder abgelaufen ist, informiert die STA das Access Gateway entsprechend und auf dem Clientgerät wird eine Fehlermeldung angezeigt.
- Nach Eingang der IP-Adresse des Computers, auf dem Citrix Presentation Server ausgeführt wird, richtet das Access Gateway eine sichere Verbindung zum Clientgerät ein. Wenn die ICA-Verbindung hergestellt ist, verschlüsselt und entschlüsselt das Access Gateway die Daten, die über die Verbindung gesendet werden.

Einrichten und Testen des Webinterface

Sie müssen das Webinterface für die Interaktion mit dem Access Gateway konfigurieren, um die Authentifizierungs- und Autorisierungsfunktionalität bereitzustellen.

Stellen Sie sicher, dass die Konfigurationseinstellungen auf dem Server, auf dem das Webinterface ausgeführt wird, korrekt die Details der STA widerspiegeln.

Beachten Sie beim Installieren und Testen des Webinterface, wenn dies mit dem Access Gateway bereitgestellt wird, die folgenden allgemeinen Hinweise.

Wichtig: Installieren und konfigurieren Sie das Webinterface, bevor Sie das Access Gateway installieren. Ausführliche Anweisungen zum Installieren des Webinterface finden Sie im *Webinterface-Administratorhandbuch*.

Konfigurieren des Webinterface

Achten Sie darauf, dass ein gültiges Serverzertifikat auf dem Access Gateway installiert ist. Weitere Informationen zum Arbeiten mit Zertifikaten finden Sie unter „Erstellen und Installieren von Zertifikaten“ auf Seite 55 und „Sichern von Verbindungen mit digitalen Zertifikaten“ auf Seite 291.

In den folgenden Schritten werden die Grundeinstellungen beschrieben, die für die gemeinsame Verwendung des Webinterface mit dem Access Gateway konfiguriert werden müssen. Weitere Informationen hierzu finden Sie im *Webinterface-Administratorhandbuch*.

So konfigurieren Sie das Webinterface für MetaFrame Presentation Server 3.0:

1. Öffnen Sie einen Webbrowser und geben Sie die folgende Webadresse ein: **http://*Servername*/Citrix/MetaFrame/WIAdmin**, wobei *Servername* der Name des Servers ist, auf dem das Webinterface ausgeführt wird.
2. Klicken Sie im linken Bereich auf **DMZ-Einstellungen** und dann auf **Netzwerkadressübersetzung**.
3. Wählen Sie **Secure Gateway-Server** und dann **Mit normaler Adresse**.
4. Klicken Sie auf **Speichern** und dann auf **Änderungen übernehmen**.
5. Klicken Sie auf **DMZ-Einstellungen** und dann auf **Secure Gateway-Unterstützung**.
6. Geben Sie den vollqualifizierten Domänennamen des Access Gateways und den Port 443 ein.
7. Fügen Sie den Server hinzu, auf dem die Secure Ticket Authority ausgeführt wird. Dieser muss mit dem im Access Gateway definierten Server identisch sein.
8. Klicken Sie auf **Speichern** und dann auf **Änderungen übernehmen**.

So konfigurieren Sie das Webinterface für Citrix Presentation Server 4.0:

1. Klicken Sie auf **Start > Programme > Citrix > MetaFrame Presentation Server > Access Suite Console für Presentation Server**.
2. Klicken Sie im linken Bereich der Access Suite Console auf **Suite-Komponenten**, klicken Sie auf **Konfigurationstools** und anschließend auf **Webinterface**.
3. Klicken Sie mit der rechten Maustaste auf die Webinterface-Site und klicken Sie dann auf **Sicheren Clientzugriff verwalten > DMZ-Einstellungen bearbeiten**.
4. Wählen Sie unter **Clientadresstabelle** den Eintrag **Standard** aus und klicken Sie dann auf **Bearbeiten**.
5. Wählen Sie im Feld **Zugriffsmethode** die Option **Secure Gateway: direkt** aus und klicken Sie zweimal auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf die Webinterface-Site und wählen Sie **Sicheren Clientzugriff verwalten > Secure Gateway-Einstellungen bearbeiten**.

7. Geben Sie im Feld **Secure Gateway-Adresse (FQDN)** den vollqualifizierten Domänennamen des Access Gateways ein. Dieser muss mit dem im Access Gateway-Zertifikat verwendeten Namen identisch sein.
8. Klicken Sie zum Aktivieren der Sitzungszuverlässigkeit auf **Sitzungszuverlässigkeit über Secure Gateway 3.0 aktivieren**.
9. Klicken Sie unter **Secure Ticket Authorities** auf **Hinzufügen**.
10. Geben Sie unter **FQDN** den Namen des Computers ein, auf dem Presentation Server ausgeführt wird, und klicken Sie auf **OK**.

So konfigurieren Sie das Webinterface für Citrix Presentation Server 4.5:

1. Klicken Sie auf **Start > Programme > Citrix > Managementkonsolen > Access Management Console**.
2. Klicken Sie im linken Bereich der Access Management Console auf **Citrix Ressourcen**, klicken Sie auf **Konfigurationstools** und anschließend auf **Webinterface**.
3. Klicken Sie mit der rechten Maustaste auf die Webinterface-Site und klicken Sie dann auf **Sicheren Clientzugriff verwalten > DMZ-Einstellungen bearbeiten**.
4. Wählen Sie unter **Clientadresstabelle** den Eintrag **Standard** aus und klicken Sie dann auf **Bearbeiten**.
5. Wählen Sie im Feld **Zugriffsmethode** die Option **Gateway: direkt** aus und klicken Sie zweimal auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf die Webinterface-Site und wählen Sie **Sicheren Clientzugriff verwalten > Gateway-Einstellungen bearbeiten**.
7. Geben Sie unter **Gateway-Server** im Feld **Adresse (FQDN)** den vollqualifizierten Domänennamen des Access Gateways ein. Dieser muss mit dem im Access Gateway-Zertifikat verwendeten Namen identisch sein.
8. Geben Sie im Feld **Port** die Portnummer ein. Der Standardwert ist 443.
9. Klicken Sie zum Aktivieren der Sitzungszuverlässigkeit auf **Sitzungszuverlässigkeit aktivieren**.
10. Klicken Sie unter **Secure Ticket Authorities** auf **Hinzufügen**.

11. Geben Sie im Feld **Secure Ticket Authority-URL** den Namen des Computers ein, auf dem Presentation Server ausgeführt wird, und klicken Sie auf **OK**.

Hinweis: Nach Abschluss dieser Schritte können nur ICA-Verbindungen über das Access Gateway gestartet werden. Richten Sie für interne Benutzer eine neue Site ein oder konfigurieren Sie Netzwerkregeln, damit die Site sowohl interne als auch externe Benutzer verarbeiten kann. Weitere Informationen hierzu finden Sie im *Webinterface-Administratorhandbuch*.

Vergewissern Sie sich nach dem Konfigurieren des Webinterface, dass die Einstellungen korrekt sind.

So überprüfen Sie die Webinterface-Einstellungen:

1. Geben Sie im Webbrowser die Webadresse des Webinterface ein (Beispiel: https://*FQDNofWebInterface/Citrix/Metaframe*).
2. Melden Sie sich am Webinterface an.
3. Klicken Sie mit der rechten Maustaste auf eine Anwendung und wählen Sie **Ziel speichern unter**.
4. Speichern Sie die Datei auf dem Desktop. Der Dateiname lautet launch.ica.
5. Klicken Sie mit der rechten Maustaste auf die Datei launch.ica und öffnen Sie sie im Editor.
6. Geben Sie an einer Eingabeaufforderung ping *AccessGatewayFQDN* ein, wobei *AccessGatewayFQDN* der Name des Access Gateways ist.
7. Doppelklicken Sie auf launch.ica.

   Wenn Sie eine SSL-Fehlermeldung erhalten, überprüfen Sie das Stammzertifikat auf dem Access Gateway und stellen Sie sicher, dass das Zertifikat ordnungsgemäß signiert ist.

Konfigurieren der Secure Ticket Authority

Beim Installieren von Citrix MetaFrame Presentation Server 3.0 wird die Secure Ticket Authority auf einem separaten Server im sicheren Netzwerk installiert und konfiguriert.

Beim Installieren von Citrix Presentation Server 4.0 für Windows wird die Secure Ticket Authority automatisch auf demselben Server wie Presentation Server im sicheren Netzwerk installiert und konfiguriert.

Wenn Presentation Server 4.0 auf einem Server installiert wird, auf dem eine ältere Version der Secure Ticket Authority vorhanden ist, wird die alte Secure Ticket Authority durch die neue Version ersetzt.

Wenn Sie die Kommunikation zwischen dem Access Gateway und der Secure Ticket Authority sichern, muss auf der Secure Ticket Authority ein Serverzertifikat installiert sein. Wenn Sie im Administration Tool auf der Registerkarte **Global Cluster Policies** das Kontrollkästchen **Validate secure certificates for internal connections** aktiviert haben, muss zur Überprüfung, ob das Zertifikat der Secure Ticket Authority gültig ist, das entsprechende Stammzertifikat auf dem Access Gateway installiert sein.

So konfigurieren Sie das Access Gateway so, dass die Secure Ticket Authority verwendet wird:

1. Klicken Sie im Administration Tool auf die Registerkarte **Authentication** und anschließend auf die Registerkarte **Secure Ticket Authority**.
2. Geben Sie unter **Server running the STA** die IP-Adresse oder den vollqualifizierten Domänennamen des Servers ein, auf dem die Secure Ticket Authority installiert ist.
3. Geben Sie unter **STA path** den Pfad zur Secure Ticket Authority ein. Der Standardpfad lautet /Scripts/CtxSTA.dll.
4. Legen Sie unter **Connection type** fest, ob die Verbindung sicher (Secure) oder unsicher (Unsecure) ist. Klicken Sie auf **Add**.

   Wenn die Secure Ticket Authority konfiguriert ist, werden der Server, der Pfad, die ID und der Verbindungstyp unter **Secure Ticket Authority Details** angezeigt.

Hinweis: Sie können der Liste mehrere Server hinzufügen, auf denen die Secure Ticket Authority ausgeführt wird. Die im Webinterface aufgelisteten Secure Ticket Authoritys müssen mit den Secure Ticket Authoritys übereinstimmen, die auf dem Access Gateway konfiguriert sind.

---

5. Klicken Sie auf die Registerkarte **Access Policy Manager**. Klicken Sie mit der rechten Maustaste entweder auf die Standardbenutzergruppe oder eine andere Gruppe und klicken Sie auf **Properties**.
6. Klicken Sie auf die Registerkarte **Gateway Portal**. Klicken Sie auf **Redirect to Web Interface**.

7. Geben Sie im Feld **Path** einen Schrägstrich (/), nichts oder die Webadresse ein, an die das Access Gateway Proxy-HTTP-Anforderungen senden soll, z. B. /Citrix/MetaFrame/auth/Login.aspx.

   Wenn dieses Feld leer gelassen oder wenn ein Schrägstrich eingegeben wird, wird die Webinterface-Standardseite verwendet.

8. Geben Sie unter **Web server** die IP-Adresse oder den vollqualifizierten Domänennamen des Servers ein, an den die Anforderungen umgeleitet werden sollen. Dies sollte die IP-Adresse des Servers sein, auf dem das Webinterface ausgeführt wird. Klicken Sie auf **OK**.

Importieren Sie nach der Konfiguration des Access Gateways ein Serverzertifikat, um eine Verbindung zur Secure Ticket Authority und zum Webinterface herstellen zu können. Dies ist erforderlich, damit Presentation Server Clients eine Verbindung zum Access Gateway herstellen können.

Wenn sich das Webinterface hinter dem Access Gateway in der DMZ oder im sicheren Netzwerk befindet, empfiehlt Citrix, dass sich Benutzer zuerst am Access Gateway anmelden, bevor sie eine Verbindung zum Webinterface herstellen.

So aktivieren Sie die Anmeldeseitenauthentifizierung:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Wählen Sie unter **Advanced options** die Option **Enable logon page authentication**.

Konfigurieren der ICA-Zugriffssteuerung

Sie können eine ICA-Zugriffssteuerungsliste konfigurieren, damit das Access Gateway nur auf bestimmte Servern in der Serverfarm Zugriff erlaubt.

Sie können im Administration Tool auf der Registerkarte **ICA Access Control**, die sich auf der Registerkarte **Authentication** befindet, eine ICA-Zugriffssteuerungsliste erstellen.

Zum Erstellen einer ICA-Zugriffssteuerungsliste müssen Sie einen IP-Adressbereich eingeben, der mit den Servern in der Serverfarm übereinstimmt, für die Sie den Zugriff gewähren wollen, und außerdem das entsprechende Protokoll bzw. den entsprechenden Port für die Verbindung mit diesen Servern festlegen.

Wenn Sie eine oder mehrere ICA-Zugriffssteuerungslisten erstellen, muss ein Server, auf dem Citrix Presentation Server ausgeführt wird, in einer der Zugriffssteuerungslisten enthalten sein, bevor Benutzer darauf zugreifen können. Das Access Gateway lässt nur Verbindungen zu den Servern zu, die in den Zugriffssteuerungslisten aufgeführt sind.

Wenn Sie keine ICA-Zugriffssteuerungsliste erstellen und die Einstellungen unter **Configure Settings for ICA Connections** auf der Registerkarte **ICA Access Control** leer lassen, wird jeglicher ICA-Verkehr durch das Access Gateway gelassen und Benutzer können mit jedem Server in der Serverfarm eine Verbindung herstellen.

So erstellen Sie eine ICA-Zugriffssteuerungsliste:

1. Klicken Sie auf der Registerkarte **Authentication** auf **ICA Access Control**.
2. Wenn Sie einen Bereich von Servern angeben möchten, auf denen Citrix Presentation Server ausgeführt wird, geben Sie in den Feldern **Starting IP address** und **Ending IP address** die erste und die letzte IP-Adresse ein.
3. Wählen Sie unter **Protocol** die Option **ICA** oder **CGP** (Citrix Gateway Protocol, das für Sitzungszuverlässigkeit verwendet wird).
4. Behalten Sie die unter **Port** angegebene Standardportnummer bei oder geben Sie eine neue Nummer ein. Der Standardport für ICA-Verbindungen ist 1494. Der Standardport für die Sitzungszuverlässigkeit ist 2598.
5. Klicken Sie auf **Add**.

Testen Sie nach dem Konfigurieren der ICA-Zugriffssteuerungsliste die Konfiguration.

So testen Sie Verbindungen zu Presentation Server:

1. Stellen Sie in einem Webbrowser mit der IP-Adresse oder dem vollqualifizierten Domänennamen eine Verbindung zum Access Gateway her.

   Die Webinterface-Anmeldeseite wird angezeigt.
2. Geben Sie Ihre Anmeldeinformationen ein und öffnen Sie dann eine Anwendung.

Wenn Sie einen Server aus dieser Liste entfernen möchten, wählen Sie den Server aus und klicken Sie dann auf **Remove**.

Verwenden des Webinterface als Anmeldeseite

Wenn Benutzer eine Verbindung zu Computern herstellen, auf denen Presentation Server ausgeführt wird, kann das Webinterface auf einem Server in der DMZ oder im Unternehmensnetzwerk installiert sein. Wenn Benutzer statt zur Access Gateway-Standardanmeldeseite eine Verbindung zum Webinterface herstellen sollen, können Sie dies auf der Registerkarte **Access Policy Manager** konfigurieren.

So konfigurieren Sie das Webinterface als Anmeldeseite:

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** unter **User Groups** auf eine Gruppe und klicken Sie dann auf **Properties**.
2. Wählen Sie auf der Registerkarte **Gateway Portal** die Option **Redirect to Web Interface**.
3. Geben Sie im Feld **Path** den Pfad des Servers ein, auf dem das Webinterface gehostet wird.
4. Geben Sie im Feld **Web server** die IP-Adresse oder den vollqualifizierten Domänennamen des Servers ein, auf dem das Webinterface gehostet wird.
5. Klicken Sie auf **Use a secure connection**, um die Verbindung zu sichern. Klicken Sie auf **OK**.

Konfigurieren von Single Sign-On beim Webinterface

Das Access Gateway kann für das Single Sign-On beim Webinterface konfiguriert werden. Dies wird auch *Passthrough-Authentifizierung* genannt. In diesem Abschnitt werden die Schritte zum Konfigurieren des Access Gateways, des Webinterface für Citrix Presentation Server 4.5, des Webinterface für Citrix Presentation Server 4.0 und des Webinterface für MetaFrame Presentation Server 3.0 für Single Sign-On beschrieben.

Dabei wird davon ausgegangen, dass das Webinterface bereits konfiguriert ist und störungsfrei mit dem Access Gateway zusammenarbeitet. Informationen zum Einrichten der Grundfunktionalität im Webinterface finden Sie unter „Konfigurieren des Webinterface für die Authentifizierung“ auf Seite 207.

Für Single Sign-On beim Webinterface müssen die folgenden Mindestvoraussetzungen erfüllt sein:

- Webinterface Version 3.0.
- Secure Ticket Authority Version 1.0 oder höher.
- Auf dem Access Gateway ist die Anmeldeseitenauthentifizierung aktiviert.
- Das Webinterface muss hinter dem Access Gateway in der DMZ oder im sicheren Netzwerk implementiert sein.
- Einzelmethodenanmeldung am Access Gateway mit LDAP-Authentifizierung Der Standardauthentifizierungsbereich muss für die Verwendung von LDAP-Authentifizierung konfiguriert sein. Bei Verwendung von RSA-, SafeWord- oder RADIUS-Authentifizierung werden die in diesem Kapitel beschriebenen Änderungen nicht unterstützt.
- Das Webinterface ist für die explizite Authentifizierung bei einer Microsoft Windows Active Directory-Domäne konfiguriert.

Neben der Erfüllung der Webinterface-Anforderungen ist es auch erforderlich, dass Presentation Server im sicheren Netzwerk installiert ist.

Das Konfigurieren des Access Gateways für die Verwendung von Passthrough-Authentifizierung hat folgende Vorteile und Funktionen:

- Benutzer müssen sich einmal beim Access Gateway authentifizieren und erhalten vom Webinterface keine Aufforderung zur erneuten Authentifizierung.
- Eingehender sicherer HTTPS-Verkehr wird vom Access Gateway beendet und authentifiziert, wobei sich das Webinterface im sicheren Netzwerk statt in der DMZ befinden kann.
- Es schützt die Server, auf denen das Webinterface ausgeführt wird.
- Es ermöglicht die Installation des Webinterface im internen Netzwerk statt in der DMZ.

Passthrough-Authentifizierung unterstützt die Anmeldung und Authentifizierung mit LDAP und Active Directory für das Access Gateway und das Webinterface.

Konfigurieren des Access Gateways für Single Sign-On beim Webinterface

Um Single Sign-On beim Webinterface zuzulassen, muss das Access Gateway auf Gruppenebene konfiguriert werden. Wenn Sie möchten, dass sich alle Gruppen mit Single Sign-On am Webinterface anmelden können, müssen Sie die Einstellungen in der Standardbenutzergruppe konfigurieren. Wenn andere Benutzergruppen die Eigenschaften der Standardbenutzergruppe erben, verwenden Benutzer in diesen Gruppen auch Passthrough-Authentifizierung.

Wichtig: Sichern Sie die Verbindung zwischen dem Access Gateway und dem Webinterface, bevor Sie diese Einstellungen aktivieren. Sonst werden Benutzeranmeldeinformationen vom Access Gateway in Klartextform an das Webinterface gesendet.

So konfigurieren Sie das Access Gateway für Single Sign-On am Webinterface:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie im linken Bereich unter **User Groups** mit der rechten Maustaste auf eine Gruppe und klicken Sie dann auf **Properties**.
3. Wählen Sie auf der Registerkarte **Gateway Portal** die Option **Redirect to Web Interface**.
4. Geben Sie unter **Path** den Pfad des Webinterface ein (z. B. /Citrix/MetaFrame/auth/login.aspx).
5. Geben Sie unter **Web server** den vollqualifizierten Domänennamen des Webinterface ein (z. B. wi.company.net).
6. Klicken Sie auf **Single sign-on to the Web Interface**.
7. Klicken Sie auf **OK**.

Konfigurieren Sie anschließend das Webinterface so, dass es die vom Access Gateway weitergeleiteten Anmeldeinformationen akzeptiert.

Konfigurieren des Webinterface für Single Sign-On

Sie können MetaFrame Presentation Server 3.0, Citrix Presentation Server 4.0 oder Citrix Presentation Server 4.5 für Single Sign-On konfigurieren. Zum Konfigurieren des Webinterface müssen folgende Aufgaben ausgeführt werden:

- Ersetzen der Datei login.cs durch eine Datei von der Citrix Support-Website
- Konfigurieren des Webinterface für Single Sign-On
- Testen der Verbindung zur Kontrolle, dass Sie sich anmelden können

So ersetzen Sie die Datei login.cs:

1. Gehen Sie auf der Citrix Support-Website (http://support.citrix.com/kb/) zum Knowledge Center-Artikel CTX106202.
2. Laden Sie die Datei AGWISSO.zip herunter und extrahieren Sie die darin enthaltenen Dateien. Sie benötigen die Datei login.cs, die sich in dieser ZIP-Datei befindet.
3. Melden Sie sich bei dem Server an, auf dem das Webinterface ausgeführt wird.
4. Navigieren Sie zu c:\Inetpub\wwwroot\Citrix\MetaFrame\site\include\serverscripts\login.cs.
5. Erstellen Sie eine Sicherungskopie der Datei login.cs.
6. Kopieren Sie die Datei login.cs, die sich in AGWISSO.zip befindet, nach c:\Inetpub\wwwroot\Citrix\MetaFrame\site\include\serverscripts\.

Wenn Sie die Datei login.cs ersetzt haben, fahren Sie mit den unten aufgeführten Arbeitsschritten zur Konfiguration des Webinterface fort. Jeder Arbeitsschritt bezieht sich speziell auf Presentation Server 3.0, Presentation Server 4.0 bzw. Presentation Server 4.5.

So konfigurieren Sie das Webinterface für MetaFrame Presentation Server 3.0 für Single Sign-On:

1. Öffnen Sie die Webinterface-Konsole, indem Sie auf **Start > Programme > Citrix > Managementkonsolen > Webinterface Console** klicken.
2. Wählen Sie im linken Bereich **Authentifizierung**.
3. Wählen Sie **Explizite Anmeldung**. Nur diese Option darf ausgewählt sein.

4. Legen Sie die Standarddomäne fest, die für die Übergabe der Anmeldeinformationen an das Webinterface verwendet werden soll. Verwenden Sie dazu eine der folgenden Methoden:
   - Definieren Sie die anzuzeigenden Domänen. Es wird die Domäne verwendet, die in der Liste an erster Stelle steht.
   - Definieren Sie nur eine Domäne und wählen Sie **Domänenfeld nicht im Anmeldeformular anzeigen**.
   - Klicken Sie auf **Speichern** und dann auf **Änderungen übernehmen**.

So konfigurieren Sie das Webinterface für Citrix Presentation Server 4.0 für Single Sign-On:

1. Klicken Sie in der Access Suite Console auf die Webinterface-Site.
2. Klicken Sie unter **Häufige Tasks** auf **Authentifizierungsmethoden konfigurieren**.
3. Wählen Sie **Explizit**.

   Stellen Sie sicher, dass nur diese Option ausgewählt ist. Vergewissern Sie sich, dass die Option **Zweifaktorauthentifizierung erzwingen** deaktiviert ist und klicken Sie dann auf **Weiter**.
4. Aktivieren Sie unter **Authentifizierungstyp** die Option **Windows oder UNIX (NIS)** und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Hinzufügen** und fügen Sie der Liste eine Domäne hinzu.

   Sind mehrere Domänen aufgeführt, verwendet das Access Gateway die Domäne, die in der Liste an erster Stelle steht.
6. Wählen Sie **Domänenfeld bei Anmeldung ausblenden**, klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**.

So konfigurieren Sie das Webinterface für Citrix Presentation Server 4.5:

1. Klicken Sie in der Access Management Console auf die Webinterface-Site.
2. Klicken Sie mit der rechten Maustaste auf die Webinterface-Site und klicken Sie dann auf **Authentifizierungsmethoden konfigurieren**.
3. Wählen Sie **Explizit** und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie unter **Explizit** auf **Authentifizierungstyp** und aktivieren Sie dann **Windows oder NIS (UNIX)**, wählen Sie **Domänenbenutzername und UPN** und klicken Sie auf **Einstellungen**.
5. Wählen Sie **Domänenfeld anzeigen** und wählen Sie unter **Domänenliste** die Option **Bereits ausgefüllt**.

6. Klicken Sie auf **Hinzufügen** und geben Sie im Feld **Anmeldedomäne** den Namen der Domäne ein.

   Sind mehrere Domänen aufgeführt, verwendet das Access Gateway die Domäne, die in der Liste an erster Stelle steht.

7. Klicken Sie dreimal auf **OK**.

Hinweis: Nach Abschluss dieser Schritte können nur ICA-Verbindungen über das Access Gateway gestartet werden. Richten Sie für interne Benutzer eine neue Site ein oder konfigurieren Sie Netzwerkregeln, damit die Site sowohl interne als auch externe Benutzer verarbeiten kann. Weitere Informationen hierzu finden Sie im *Webinterface-Administratorhandbuch*.

Vergewissern Sie sich nach dem Konfigurieren des Webinterface, dass Sie sich anmelden können.

So testen Sie Single Sign-On am Webinterface:

1. Geben Sie in einem Webbrowser **https://*AccessGatewayFQDN*** ein, wobei *AccessGatewayFQDN* der vollqualifizierte Domänenname (FQDN) des Access Gateways ist.
2. Melden Sie sich mit denselben Benutzeranmeldeinformationen wie in Active Directory an.

   Bei der Anmeldung werden Sie zum Webinterface in der Standardgruppe oder der Gruppe mit der höchsten Priorität, der der Benutzer angehört, weitergeleitet.

   Die Anwendungen werden ohne weitere Authentifizierung automatisch angezeigt. Beim Starten einer veröffentlichten Anwendung sollte der Presentation Server Client den Verkehr durch das Access Gateway-Gerät an Server in der Farm weiterleiten.

Aktivieren der Sitzungszuverlässigkeit

Die Sitzungszuverlässigkeit hält ICA-Sitzungen aktiv und sorgt dafür, dass sie auf dem Bildschirm des Benutzers verbleiben, wenn die Netzwerkverbindung unterbrochen ist.

Die Sitzungszuverlässigkeit wird unter Verwendung der Secure Gateway 3.0-Einstellungen im Webinterface in der Citrix Access Management Console konfiguriert. Öffnen Sie zum Aktivieren der Sitzungszuverlässigkeit Port 2598 in der internen Firewall.

So aktivieren Sie die Sitzungszuverlässigkeit im Webinterface:

1. Klicken Sie in der Access Management Console unter **Webinterface** auf die Webinterface-Site.
2. Klicken Sie unter **Häufige Tasks** auf **Sicheren Clientzugriff verwalten** und dann auf **Gateway-Einstellungen bearbeiten**.
3. Geben Sie im Dialogfeld **Gateway-Einstellungen bearbeiten** unter **Gateway-Server** im Feld **Adresse (FQDN)** die IP-Adresse oder den vollqualifizierten Domänennamen des Access Gateways ein.
4. Geben Sie unter **Port** die Portnummer ein. Der Standardwert ist 443.
5. Aktivieren Sie die Option **Sitzungszuverlässigkeit aktivieren**. Klicken Sie auf **OK**.

Bereitstellen des Access Gateways in einer Double-Hop-DMZ

Einige Unternehmen verwenden drei Firewalls zum Schutz ihrer internen Netzwerke. Diese drei Firewalls unterteilen die DMZ in zwei Bereiche, sodass ein zusätzliches Maß an Sicherheit für das interne Netzwerk erzielt wird. Diese Netzwerkkonfiguration wird als *Double-Hop-DMZ* bezeichnet.

Access Gateway-Geräte in einer Double-Hop-DMZ

Sie können Access Gateway-Geräte in einer Double-Hop-DMZ bereitstellen, um den Zugriff auf Server zu steuern, auf denen Citrix Presentation Server ausgeführt wird, wie in der Abbildung oben dargestellt.

In einer Double-Hop-DMZ-Bereitstellung stellen Benutzer mit einem Webbrowser und einem Citrix Presentation Server Client eine Verbindung zum Access Gateway in der ersten DMZ her.

Dieser Vorgang wird gestartet, indem der Benutzer über einen Webbrowser eine Verbindung zum Access Gateway herstellt und im Webinterface eine veröffentlichte Anwendung auswählt. Nach Auswahl einer veröffentlichten Anwendung wird der Citrix Presentation Server Client automatisch auf dem Clientgerät gestartet. Der Presentation Server Client stellt eine Verbindung zum Access Gateway her, um auf die veröffentlichte Anwendung zuzugreifen, die auf der Serverfarm im sicheren Netzwerk ausgeführt wird.

Wichtig: Der Secure Access Client wird in Double-Hop-DMZ-Bereitstellungen nicht unterstützt. Sie können mit dem Secure Access Client also nicht auf Netzwerkressourcen zugreifen, wenn das Access Gateway in einer Double-Hop-DMZ-Konfiguration bereitgestellt wurde.

Das Access Gateway in der ersten DMZ ist für Clientverbindungen verantwortlich und übernimmt die Sicherheitsfunktionen eines SSL-VPN. Dieses Access Gateway verschlüsselt die Clientverbindungen, legt fest, wie Clients authentifiziert werden, und steuert den Zugriff auf die Server, auf denen Citrix Presentation Server im internen Netzwerk ausgeführt wird.

Das Access Gateway in der zweiten DMZ ist ein Proxygerät. Dieses Access Gateway stellt Presentation Server Client-Verbindungen mit der Serverfarm her, indem es ICA-Datenübertragungen das Durchqueren der zweiten DMZ ermöglicht. Die Datenübertragung zwischen dem Access Gateway in der ersten DMZ und der Secure Ticket Authority im internen Netzwerk erfolgt auch über das Access Gateway in der zweiten DMZ.

Hinweis: Der Begriff *Access Gateway-Proxy* bezieht sich auf ein Access Gateway-Gerät, das in der zweiten DMZ bereitgestellt wird.

In diesem Kapitel werden die folgenden Themen zur Bereitstellung des Access Gateways in einer Konfiguration mit einer Double-Hop-DMZ behandelt:

- Datenübertragung in einer Double-Hop-DMZ-Konfiguration: In diesem Abschnitt wird kurz erläutert, wie die Datenübertragung zwischen den verschiedenen Komponenten in einer Double-Hop-DMZ abläuft.
- Vorbereiten der Bereitstellung einer Double-Hop-DMZ: In diesem Abschnitt werden die Konfigurationsaspekte erläutert, die Sie vor dem Bereitstellen von Access Gateway-Geräten in einer Double-Hop-DMZ berücksichtigen sollten.

- Erforderliche Schritte zur Bereitstellung einer Double-Hop-DMZ: In diesem Abschnitt wird beschrieben, welche Arbeitsschritte zum Bereitstellen von Access Gateway-Geräten in einer Double-Hop-DMZ-Konfiguration erforderlich sind.
- Herstellen einer Clientverbindung in einer Double-Hop-DMZ: Dieser Abschnitt enthält eine detaillierte Beschreibung der einzelnen Schritte zur Herstellung einer Clientverbindung und der Interaktion zwischen den verschiedenen Komponenten in einer Double-Hop-DMZ-Bereitstellung.

Datenübertragung in einer Double-Hop-DMZ-Konfiguration

In diesem Abschnitt wird die Datenübertragung erläutert, die bei einer Clientverbindung zwischen den verschiedenen Komponenten in einer Double-Hop-DMZ abläuft. Um zu verstehen, welche Konfigurationsaspekte bei der Bereitstellung einer Double-Hop-DMZ zu berücksichtigen sind, sollten Sie grundsätzlich wissen, wie die Kommunikation zwischen den verschiedenen Komponenten in einer Double-Hop-DMZ erfolgt.

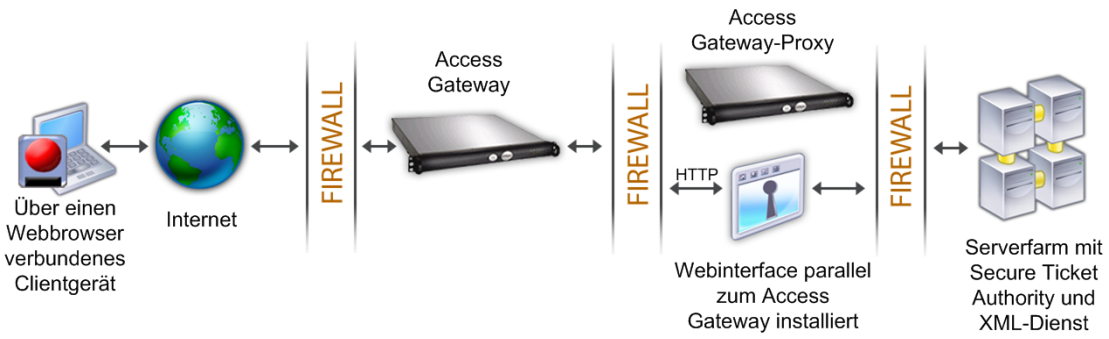
Der Datenübertragung zwischen den Komponenten wird in drei separaten Phasen beschrieben:

- Clientauthentifizierung
- Erstellung von Sitzungstickets
- Verbindungsherstellung

Hinweis: Eine detailliertere Beschreibung dieses Prozesses finden Sie unter „Herstellen einer Clientverbindung in einer Double-Hop-DMZ“ auf Seite 250.

Clientauthentifizierung

Die Clientauthentifizierung ist die erste Phase beim Herstellen einer Clientverbindung in einer Double-Hop-DMZ-Bereitstellung.



Datenübertragung bei der Clientauthentifizierung in einer Double-Hop-DMZ

Während der Clientauthentifizierungsphase laufen die folgenden Schritte ab:

- Ein Benutzer stellt über einen Webbrowser eine Verbindung zum Access Gateway in der ersten DMZ her. Wenn auf dem Access Gateway die Anmeldeseitenauthentifizierung aktiviert ist, wird der Benutzer vom Access Gateway authentifiziert.
- Das Access Gateway leitet die Webbrowser-Verbindung an das Webinterface weiter.
- Das Webinterface kommuniziert mit dem XML-Dienst auf einem Server, auf dem Citrix Presentation Server ausgeführt wird, und erhält vom XML-Dienst eine Liste der Anwendungen, auf die der Benutzer zugreifen darf. Bei diesem Prozess wird der Benutzer vom XML-Dienst authentifiziert.

Erstellung von Sitzungstickets

Die Erstellung von Sitzungstickets ist die zweite Phase beim Herstellen einer Clientverbindung in einer Double-Hop-DMZ-Bereitstellung.

Während dieser Phase laufen die folgenden Schritte ab:

- Das Webinterface kommuniziert mit dem XML-Dienst und der Secure Ticket Authority im internen Netzwerk, um Sitzungstickets für die einzelnen veröffentlichten Anwendungen zu erstellen, auf die der Benutzer zugreifen darf.

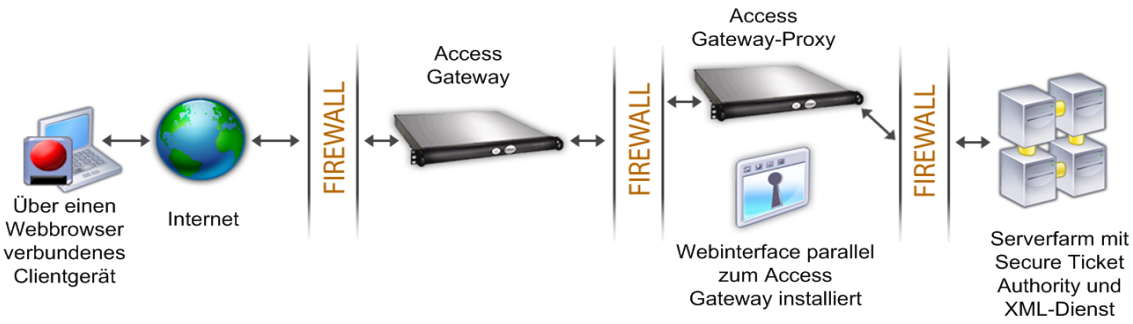
  Das Sitzungsticket enthält eine Aliasadresse für den Computer, auf dem Presentation Server ausgeführt wird und der eine veröffentlichte Anwendung hostet.

- Das Webinterface erstellt eine ICA-Datei für jede veröffentlichte Anwendung. Jede ICA-Datei enthält das Sitzungsticket für eine veröffentlichte Anwendung.

- Das Webinterface erstellt eine Webseite mit einem Link zu jeder veröffentlichten Anwendung (ICA-Datei), auf die der Benutzer zugreifen darf, und leitet diese Webseite an den Clientbrowser weiter.

Verbindungsherstellung

Die endgültige Herstellung der Verbindung ist die dritte Phase beim Herstellen einer Clientverbindung in einer Double-Hop-DMZ-Bereitstellung.



Datenübertragung bei der Verbindungsherstellung in einer Double-Hop-DMZ

Während dieser Phase, in der die Verbindung endgültig hergestellt wird, laufen die folgenden Schritte ab:

- Der Benutzer klickt auf der vom Webinterface bereitgestellten Webseite auf einen Link zu einer veröffentlichten Anwendung.
- Der Webbrowser erhält die vom Webinterface erstellte ICA-Datei und startet den Citrix Presentation Server Client.

Hinweis: Die ICA-Datei enthält Anweisungen für den Webbrowser zum Starten des Presentation Server Clients.

- Der Presentation Server Client stellt eine ICA-Verbindung zum Access Gateway in der ersten DMZ her.
- Das Access Gateway in der ersten DMZ kommuniziert mit der Secure Ticket Authority im internen Netzwerk, um die im Sitzungsticket enthaltene Aliasadresse in die echte IP-Adresse eines Computers aufzulösen, auf dem Presentation Server ausgeführt wird. Diese Datenübertragung erfolgt über die zweite DMZ durch den Access Gateway-Proxy.
- Dann wird eine Verbindung vom Access Gateway in der zweiten DMZ zu dem Server im internen Netzwerk hergestellt, auf dem Presentation Server ausgeführt wird.
- Das Access Gateway in der ersten DMZ stellt eine endgültige ICA-Verbindung zum Presentation Server Client her.

  Jetzt kann der Presentation Server Client über beide Access Gateway-Geräte mit dem Computer im internen Netzwerk kommunizieren, auf dem Presentation Server ausgeführt wird.

Vorbereiten der Bereitstellung einer Double-Hop-DMZ

Zur Vorbereitung der Bereitstellung einer Double-Hop-DMZ sollten Sie als erstes die folgenden Fragen klären. Durch die Beantwortung dieser Fragen vor der Implementierung können Sie unnötige Probleme bei der Bereitstellung vermeiden.

- Soll Lastausgleich unterstützt werden?
- Soll die Anmeldeseitenauthentifizierung auf dem Access Gateway aktiviert werden?
- Wo soll das Administration Tool installiert werden?

- Welche Ports müssen in den Firewalls geöffnet werden?
- Wie viele SSL-Zertifikate sind erforderlich?
- Welche Komponenten sind vor dem Starten der Bereitstellung erforderlich?

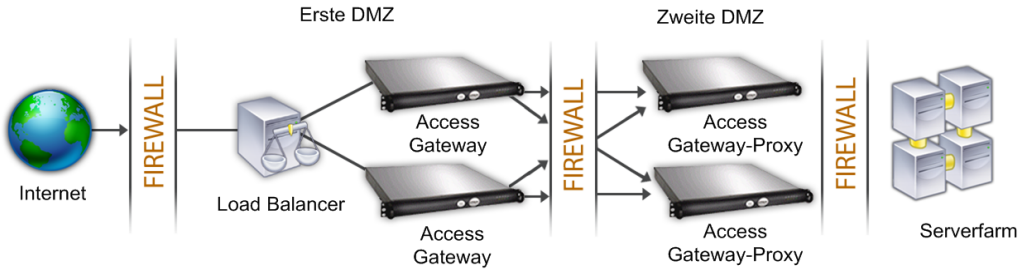
Anhand der in diesem Abschnitt enthaltenen Informationen können Sie diese Fragen für Ihre spezielle Umgebung leichter beantworten.

Unterstützen von Lastausgleich

Bevor Sie mit der Bereitstellung einer Double-Hop-DMZ beginnen, sollten Sie entscheiden, ob in Ihrer Double-Hop-DMZ Lastausgleich unterstützt werden soll.

Die Unterstützung von Lastausgleich bietet folgende Vorzüge:

- Sie können mehrere Access Gateway-Geräte in jeder DMZ bereitstellen, um zu gewährleisten, dass die Access Gateway-Bereitstellung keinen SPoF (Single Point of Failure, d. h. keine einzelne Fehlerstelle) hat. Wenn ein Access Gateway ausfällt, steht ein anderes Access Gateway für die Benutzerverbindungen zur Verfügung.
- Zur Optimierung der Leistung für den Endbenutzer werden die Benutzerverbindungen gleichmäßig auf die verschiedenen Access Gateway-Geräte verteilt.



Zwei in der ersten DMZ und zwei in der zweiten DMZ bereitgestellte Access Gateway-Geräte zur Gewährleistung hoher Verfügbarkeit

Wenn Sie mehrere Geräte in der ersten DMZ bereitstellen, müssen Sie einen Load Balancer vor diesen Geräten implementieren. Beim Konfigurieren des Lastausgleichs für die Access Gateway-Geräte in der ersten DMZ können Sie genauso vorgehen wie bei jeder anderen Access Gateway-Bereitstellung. Weitere Informationen zum Konfigurieren von Lastausgleich finden Sie unter „Installieren zusätzlicher Access Gateway-Geräte“ auf Seite 271.

Wenn Sie mehrere Geräte in der zweiten DMZ bereitstellen, können Sie jedes Access Gateway in der ersten DMZ so konfigurieren, dass eine Verbindung zu jedem Access Gateway-Proxygerät in der zweiten DMZ hergestellt werden kann.

Wenn ein Access Gateway in der ersten DMZ eine Verbindung zu mehreren Access Gateway-Geräten in der zweiten DMZ herstellt, führt das Access Gateway in der ersten DMZ einen Lastausgleich nach dem Round-Robin-Prinzip für die Verbindungen zu den Geräten in der zweiten DMZ aus. Durch diesen Lastausgleich ist gewährleistet, dass die Verbindungen gleichmäßig auf die Geräte in der zweiten DMZ verteilt sind. Wenn ein Access Gateway-Gerät in der zweiten DMZ ausfällt, dann wird die Verbindung zu einem anderen, noch verfügbaren Access Gateway in der zweiten DMZ hergestellt.

Informationen zum Konfigurieren eines Access Gateways, um eine Verbindung zu mehreren Access Gateway-Proxygeräten herzustellen, finden Sie unter „Schritt 5: Konfigurieren des Access Gateways für die Kommunikation mit dem Access Gateway-Proxy“ auf Seite 239.

Verwenden der Anmeldeseitenauthentifizierung in einer Double-Hop-DMZ

Vor dem Bereitstellen von Access Gateway-Geräten in einer Double-Hop-DMZ sollten Sie entscheiden, ob die Anmeldeseitenauthentifizierung auf dem (den) Access Gateway-Gerät(en) in der ersten DMZ aktiviert oder deaktiviert werden soll.

Über die Konfiguration der Anmeldeseitenauthentifizierung auf dem Access Gateway in der ersten DMZ wird gesteuert, wie Benutzer authentifiziert werden. Außerdem wirkt sich dies auch auf andere Sicherheitskonfigurationen in der Umgebung aus. Wenn Sie vor dem Starten der Bereitstellung verstehen, wie sich die Anmeldeseitenauthentifizierung auswirkt, können Sie Probleme mit Sicherheitskonfigurationen in Ihrer Umgebung bei der tatsächlichen Bereitstellung vermeiden.

- Die Aktivierung der Anmeldeseitenauthentifizierung erhöht die Sicherheit, setzt aber auch voraus, dass Sie auf dem Access Gateway in der ersten DMZ einen Authentifizierungsbereich erstellen und die Funktion für das Single Sign-On am Webinterface aktivieren.
- Die Deaktivierung der Anmeldeseitenauthentifizierung ist zwar leichter zu konfigurieren, bietet jedoch geringere Sicherheit.

Diese Optionen werden nachstehend jeweils näher erläutert.

Aktivieren der Anmeldeseitenauthentifizierung

Wenn Sie die Anmeldeseitenauthentifizierung auf dem Access Gateway in der ersten DMZ aktivieren, wird eine Benutzerverbindung sowohl vom Access Gateway als auch vom XML-Dienst auf einem Computer authentifiziert, auf dem Citrix Presentation Server ausgeführt wird. Die Aktivierung der Anmeldeseitenauthentifizierung erhöht die Sicherheit, weil der Benutzer vor dem Zugriff auf veröffentlichte Anwendungen zweimal authentifiziert wird.

Wenn Sie die Anmeldeseitenauthentifizierung aktivieren, werden Benutzer zur Eingabe ihrer Authentifizierungsinformationen (Benutzername und Kennwort) aufgefordert, wenn Sie über einen Webbrowser eine Verbindung zum Access Gateway in der ersten DMZ herstellen. Zur Unterstützung dieser Benutzerauthentifizierung müssen Sie einen Authentifizierungsbereich auf dem Access Gateway erstellen. Weitere Informationen zum Erstellen von Authentifizierungsbereichen finden Sie unter „Konfigurieren der Authentifizierung auf dem Access Gateway“ auf Seite 78.

Hinweis: Der Authentifizierungsbereich dient zur Authentifizierung des Benutzers, gewährt dem Benutzer jedoch keinen Zugriff auf die Serverfarm. Wenn Sie einen Authentifizierungsbereich auf dem Access Gateway in der ersten DMZ erstellen, aktivieren Sie die Option **No authorization** als Autorisierungstyp.

In einer Double-Hop-DMZ-Bereitstellung erfolgt die Autorisierung über das Webinterface/den XML-Dienst und die ICA-Zugriffssteuerungsliste, die auf dem Access Gateway in der ersten DMZ konfiguriert ist. Die zur Unterstützung der Autorisierung erforderlichen Einstellungen werden weiter unten in diesem Kapitel erläutert.

Wenn Sie die Anmeldeseitenauthentifizierung aktivieren, sollten Sie auch die Access Gateway-Option für Single Sign-On am Webinterface aktivieren.

Beim Aktivieren von Single Sign-On wird der Benutzer zweimal authentifiziert, gibt seine Authentifizierungsinformationen allerdings nur einmal ein. Das Access Gateway authentifiziert den Benutzer und leitet seine Anmeldeinformationen an das Webinterface weiter. Das Webinterface leitet die Anmeldeinformationen an den XML-Dienst weiter, wobei der Benutzer nicht zur erneuten Eingabe seiner Anmeldeinformationen aufgefordert wird. Der XML-Dienst authentifiziert den Benutzer und legt fest, auf welche veröffentlichten Anwendungen der Benutzer zugreifen darf.

Zum Aktivieren von Single Sign-On müssen das Access Gateway und das Webinterface den Benutzer über denselben Authentifizierungsserver (z. B. denselben LDAP- oder RADIUS-Server) authentifizieren.

Wenn Sie die Anmeldeseitenauthentifizierung, jedoch nicht die Option für Single Sign-On am Webinterface aktivieren, ist Folgendes zu beachten:

- Für den Zugriff auf veröffentlichte Anwendungen muss der Benutzer seine Anmeldeinformationen zweimal eingeben. Der Benutzer gibt seine Authentifizierungsinformationen zuerst auf der Access Gateway-Anmeldeseite und dann erneut auf der Webinterface-Anmeldeseite ein.
- Das Access Gateway und das Webinterface können den Benutzer über verschiedene Authentifizierungsserver authentifizieren.

Wenn Sie die Anmeldeseitenauthentifizierung aktivieren, müssen Sie auch sicherstellen, dass die entsprechenden Ports in den Firewalls offen sind, damit das Access Gateway in der ersten DMZ mit dem Authentifizierungsserver kommunizieren kann.

Wenn sich beispielsweise ein RADIUS-Server im internen Netzwerk befindet und Port 1812 nach Authentifizierungsverbindungen abhört, müssen Sie diesen Port durch die zweite und dritte Firewall öffnen, damit das Access Gateway in der ersten DMZ mit dem Authentifizierungsserver kommunizieren kann.

Deaktivieren der Anmeldeseitenauthentifizierung

Wenn Sie die Anmeldeseitenauthentifizierung auf dem Access Gateway in der ersten DMZ deaktivieren, wird der Benutzer zwar vom XML-Dienst, jedoch nicht vom Access Gateway authentifiziert. Diese Option ist zwar leichter zu konfigurieren, bietet jedoch geringere Sicherheit, weil der Benutzer vor dem Zugriff auf die veröffentlichten Anwendungen nur einmal authentifiziert wird.

Wenn Sie die Anmeldeseitenauthentifizierung deaktivieren, laufen folgende Schritte ab:

- Der Benutzer stellt über einen Webbrowser eine Verbindung zum Access Gateway her.
- Das Access Gateway ruft die Anmeldeseite vom Webinterface ab und zeigt dem Benutzer diese Anmeldeseite an.
- Der Benutzer gibt seine Authentifizierungsinformationen ein, die vom Access Gateway an das Webinterface weitergeleitet werden.
- Das Webinterface leitet die Anmeldeinformationen zur Authentifizierung an den XML-Dienst weiter.

Wenn die Anmeldeseitenauthentifizierung deaktiviert ist, wird die Access Gateway-Anmeldeseite nicht verwendet; das Access Gateway nimmt auch keine Authentifizierung vor. Sie müssen keinen Authentifizierungsbereich auf dem Access Gateway konfigurieren.

Planen der Installation des Access Gateway Administration Tools

Vor dem Bereitstellen des Access Gateways in einer Double-Hop-DMZ sollten Sie entscheiden, wo das Access Gateway Administration Tool installiert werden soll. Wenn Sie die Installation des Administration Tools im Voraus planen, können Sie Verbindungsprobleme während der Bereitstellung vermeiden.

Zum Installieren und Verwenden des Administration Tools auf einem Computer muss dieser Computer zwei Verbindungen zu einem Access Gateway herstellen. Standardmäßig werden diese Verbindungen auf den folgenden TCP-Ports hergestellt:

- Port 9001: An diesem Port stellt ein Webbrowser eine Verbindung zum Administration Portal her. Zum Herunterladen und Installieren des Administration Tools müssen Sie eine Verbindung zum Administration Portal herstellen.
- Port 9002: An diesem Port stellt das Administration Tool eine Verbindung zum Access Gateway her, wenn Sie Änderungen an den Access Gateway-Verwaltungseinstellungen vornehmen.

Zum Installieren und Verwenden des Administration Tools müssen Sie diese Ports an einer Firewall öffnen, die sich zwischen dem Access Gateway und dem Computer befindet, der als Host für das Administration Tool fungieren soll.

Bei der Bereitstellung einer Double-Hop-DMZ ist es u. U. leichter, das Administration Tool in der zweiten DMZ auf dem gleichen Computer zu installieren, der als Host für das Webinterface fungiert (oder auf einem anderen Computer, der sich in der zweiten DMZ befindet). Wenn Sie das Administration Tool in der zweiten DMZ installieren, können Sie sämtliche Access Gateways und Access Gateway-Proxygeräte in der Bereitstellung über dieses Administration Tool verwalten.

Wenn Sie das Administration Tool auf dem Webinterface-Computer (oder einem anderen Computer in der zweiten DMZ) installieren möchten, ist Folgendes zu beachten:

- Öffnen Sie Ports 9001 und 9002 in der Firewall zwischen der ersten und der zweiten DMZ, bevor Sie mit der Bereitstellung der Double-Hop-DMZ beginnen. Diese Ports müssen offen sein, damit die zur Installation des Administration Tools auf einem Computer in der zweiten DMZ erforderlichen Verbindungen hergestellt werden können.
- Installieren Sie das Administration Tool zur gleichen Zeit, wie Sie das erste Access Gateway in der ersten DMZ installieren. (Nähere Anweisungen zum Installieren des Administration Tools finden Sie unter „Konfigurieren der TCP/IP-Einstellungen mit Netzwerkkabeln“ auf Seite 45.)
- Beim Installieren weiterer Access Gateway-Geräte in der ersten und zweiten DMZ bei der Bereitstellung einer Double-Hop-DMZ verwenden Sie dieses Administration Tool zum Erstellen eines Access Gateway-Clusters mit allen Geräten, die in der Double-Hop-DMZ installiert sind. Über dieses Administration Tool können Sie dann administrative

Änderungen an sämtlichen Access Gateway-Geräten in der Double-Hop-DMZ vornehmen.

Hinweis: Über die Registerkarte **Access Gateway Cluster** können Sie dem Cluster weitere Geräte hinzufügen. Weitere Informationen hierzu finden Sie unter „Erstellen eines Clusters mit Access Gateway-Geräten“ auf Seite 273.

Öffnen von Ports und Verwalten von Zertifikaten

In einer Double-Hop-DMZ werden unterschiedliche Verbindungen zwischen den verschiedenen Komponenten hergestellt.

Vor dem Bereitstellen von Access Gateway-Geräten in einer Double-Hop-DMZ sollten Sie verstehen, welche Verbindungen zwischen den einzelnen Komponenten in einer Double-Hop-DMZ hergestellt werden, welche Ports von diesen Verbindungen verwendet werden und welche Zertifikate zur Verschlüsselung dieser Verbindungen notwendig sind.

Die Aspekte, die mit dem Öffnen von Ports und Installieren von Zertifikaten verknüpft sind, werden weiter unten in den Anweisungen zum Bereitstellen von Access Gateway-Geräten in einer Double-Hop-DMZ erläutert. Wenn Sie sich vor der Bereitstellung mit firewall- und zertifikatspezifischen Aspekten vertraut machen möchten, finden Sie nähere Informationen an folgenden Stellen:

- „Schritt 8: Öffnen der entsprechenden Ports in den Firewalls“ auf Seite 244.
- „Schritt 9: Verwalten von SSL-Zertifikaten in einer Double-Hop-DMZ-Bereitstellung“ auf Seite 246.

Für die Bereitstellung erforderliche Komponenten

Bevor Sie mit der Bereitstellung einer Double-Hop-DMZ beginnen, müssen die folgenden Komponenten vorhanden sein:

- Mindestens zwei Access Gateway-Geräte (ein Gerät pro DMZ) müssen vorhanden sein.

  Wenn Sie zur Unterstützung von Lastausgleich mehrere Geräte in jeder DMZ installieren möchten, sind weitere Access Gateway-Geräte erforderlich. Weitere Informationen hierzu finden Sie unter „Unterstützen von Lastausgleich“ auf Seite 229.

- Die Server, auf denen Citrix Presentation Server ausgeführt wird, müssen im internen Netzwerk installiert und betriebsbereit sein.

- Das Webinterface muss in der zweiten DMZ installiert und für den Betrieb mit der Serverfarm im internen Netzwerk konfiguriert sein.
- Es muss mindestens ein SSL-Serverzertifikat vorhanden sein, um es auf dem Access Gateway in der ersten DMZ zu installieren. Dieses Zertifikat gewährleistet, dass die Verbindungen vom Webbrowser und Presentation Server Client zum Access Gateway verschlüsselt werden.

  Wenn Sie Verbindungen zwischen den anderen Komponenten einer Double-Hop-DMZ-Bereitstellung verschlüsseln möchten, sind weitere Zertifikate erforderlich. Weitere Informationen hierzu finden Sie unter „Schritt 9: Verwalten von SSL-Zertifikaten in einer Double-Hop-DMZ-Bereitstellung“ auf Seite 246.

Installieren des Access Gateways in einer Double-Hop-DMZ

In diesem Abschnitt werden die Arbeitsschritte erläutert, die zum Bereitstellen des Access Gateways in einer Double-Hop-DMZ erforderlich sind.

Dazu zählen die folgenden Schritte:

- Schritt 1: Installieren eines Access Gateway-Geräts in der ersten DMZ
- Schritt 2: Aktivieren oder Deaktivieren der Anmeldeseitenauthentifizierung
- Schritt 3: Konfigurieren des Access Gateways zur Weiterleitung von Verbindungen an das Webinterface
- Schritt 4: Installieren eines Access Gateway-Geräts in der zweiten DMZ
- Schritt 5: Konfigurieren des Access Gateways für die Kommunikation mit dem Access Gateway-Proxy
- Schritt 6: Konfigurieren des Access Gateway-Proxy für die Kommunikation mit dem Access Gateway
- Schritt 7: Konfigurieren des Access Gateways für den Secure Ticket Authority- und ICA-Datenverkehr
- Schritt 8: Öffnen der entsprechenden Ports in den Firewalls
- Schritt 9: Verwalten der SSL-Zertifikate

Schritt 1: Installieren eines Access Gateways in der ersten DMZ

Nachstehend finden Sie die Anweisungen zur Installation eines Access Gateway-Geräts in der ersten DMZ einer Double-Hop-DMZ und Probleme, die dabei auftreten können:

- Folgen Sie den Anweisungen unter „Erstmalige Installation des Access Gateways“ auf Seite 39, um das Access Gateway-Gerät in der ersten DMZ zu installieren.
- Beim Installieren eines Access Gateways in der ersten DMZ konfigurieren Sie dieses zur Verwendung von Interface 0 und Interface 1. Verbinden Sie Interface 0 mit dem Internet (oder einem anderen externen Netzwerk) und Interface 1 mit der zweiten DMZ.
- Während der Installation des Access Gateways installieren Sie das Access Gateway Administration Tool. Vor dem Installationsbeginn finden Sie unter „Planen der Installation des Access Gateway Administration Tools“ auf Seite 232 nähere Informationen zur Verwendung des Administration Tools in einer Double-Hop-DMZ-Bereitstellung.
- Wenn Sie mehrere Access Gateway-Geräte in der ersten DMZ installieren, können Sie diese Geräte hinter einem Load Balancer bereitstellen. Weitere Informationen hierzu finden Sie unter „Unterstützen von Lastausgleich“ auf Seite 229.

Schritt 2: Aktivieren oder Deaktivieren der Anmeldeseitenauthentifizierung

Bei diesem Schritt haben Sie auf dem Access Gateway in der ersten DMZ folgenden Möglichkeiten:

- Aktivieren Sie die Anmeldeseitenauthentifizierung, damit Benutzer sowohl vom Access Gateway als auch vom XML-Dienst authentifiziert werden.
- Deaktivieren Sie die Anmeldeseitenauthentifizierung, damit Benutzer nur vom XML-Dienst authentifiziert werden.

Nähere Informationen zu den Auswirkungen der Aktivierung bzw. Deaktivierung der Anmeldeseitenauthentifizierung finden Sie unter „Verwenden der Anmeldeseitenauthentifizierung in einer Double-Hop-DMZ“ auf Seite 230.

So aktivieren oder deaktivieren Sie die Anmeldeseitenauthentifizierung:

1. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
2. Aktivieren oder deaktivieren Sie unter **Advanced options** die Option **Enable logon page authentication**.
3. Klicken Sie auf **Submit**.

Wenn Sie die Anmeldeseitenauthentifizierung aktivieren, sollten Sie auch die Option für Single Sign-On am Webinterface aktivieren. Nähere Anweisungen zum Aktivieren von Single Sign-On finden Sie unter “Schritt 3: Konfigurieren des Access Gateways zur Weiterleitung von Verbindungen an das Webinterface”.

Schritt 3: Konfigurieren des Access Gateways zur Weiterleitung von Verbindungen an das Webinterface

In einer Double-Hop-DMZ-Bereitstellung müssen Sie jedes Access Gateway in der ersten DMZ so konfigurieren, dass Verbindungen zum Webinterface in der zweiten DMZ weitergeleitet werden.

Die Weiterleitung an das Webinterface erfolgt auf Benutzergruppenebene. Für die Herstellung einer Verbindung zum Webinterface über das Access Gateway muss der Benutzer mit einer Access Gateway-Benutzergruppe (z. B. der Gruppe **Default**) verknüpft sein, bei der die Weiterleitung an das Webinterface aktiviert ist.

Wichtig: Single Sign-On am Webinterface wird ebenfalls auf Benutzergruppenebene konfiguriert. Wenn Sie die Anmeldeseitenauthentifizierung im vorigen Schritt aktiviert haben, sollten Sie auch die Option für Single Sign-On am Webinterface aktivieren.

So leiten Sie Verbindungen an das Webinterface weiter:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste auf die Benutzergruppe **Default** und klicken Sie auf **Properties**.
3. Klicken Sie auf die Registerkarte **Gateway Portal**. Klicken Sie auf **Redirect to Web Interface**.

4. Geben Sie unter **Path** wahlweise Folgendes ein:

   - Geben Sie die spezielle Webadresse ein, an die das Access Gateway HTTP-Anforderungen weiterleiten soll. (Die Standardeinstellung ist /Citrix/MetaFrame/auth/Login.aspx.)
   - Geben Sie einen Schrägstrich (/) ein oder lassen Sie das Feld leer, damit Anforderungen an die Webinterface-Standardseite weitergeleitet werden.

5. Geben Sie im Feld **Web server** die IP-Adresse oder den vollqualifizierten Domänennamen des Servers ein, auf dem das Webinterface ausgeführt wird.

6. (Optional) Aktivieren Sie die Option **Single sign-on to the Web Interface**, wenn Sie die Anmeldeseitenauthentifizierung aktiviert haben. Aktivieren Sie diese Option nicht, wenn die Anmeldeseitenauthentifizierung deaktiviert ist.

   Weitere Informationen hierzu finden Sie unter „Verwenden der Anmeldeseitenauthentifizierung in einer Double-Hop-DMZ“ auf Seite 230.

7. (Optional) Aktivieren Sie die Option **Use a secure connection**, wenn die Verbindung vom Access Gateway zum Webinterface mit SSL verschlüsselt werden soll. Klicken Sie auf **OK**.

   Hinweis: Wenn Sie die Option **Use a secure connection** aktivieren, müssen Sie die entsprechenden SSL-Zertifikate installieren. Weitere Informationen finden Sie unter „Schritt 9: Verwalten von SSL-Zertifikaten in einer Double-Hop-DMZ-Bereitstellung“ auf Seite 246.

   ---

8. Wiederholen Sie diese Schritte für jedes Access Gateway, das in der ersten DMZ installiert ist.

Schritt 4: Installieren eines Access Gateways in der zweiten DMZ

Das Access Gateway-Gerät in der zweiten DMZ wird als *Access Gateway-Proxy* bezeichnet, da es als Proxy für den ICA- und Secure Ticket Authority-Datenverkehr durch die zweite DMZ fungiert.

Folgen Sie den Anweisungen unter „Erstmalige Installation des Access Gateways“ auf Seite 39, um die einzelnen Access Gateway-Geräte in der zweiten DMZ zu installieren.

Beim Installieren eines Access Gateways in der ersten DMZ konfigurieren Sie dieses zur Verwendung von Interface 0 und Interface 1. Verbinden Sie Interface 0 mit der ersten DMZ und Interface 1 mit dem internen Netzwerk, das die Serverfarm enthält.

Bei der Installation weiterer Geräte in der zweiten DMZ können Sie genauso vorgehen. Nähere Informationen zum Verwenden mehrerer Access Gateway-Geräte zur Gewährleistung hoher Verfügbarkeit finden Sie unter „Unterstützen von Lastausgleich“ auf Seite 229.

Wenn das Access Gateway in der zweiten DMZ installiert ist, müssen Sie das Administration Tool installieren oder das Gerät mit einem bereits installierten Administration Tool einem Cluster hinzufügen. Nähere Informationen zur Verwendung des Administration Tools in einer Double-Hop-DMZ-Bereitstellung finden Sie unter„Planen der Installation des Access Gateway Administration Tools“ auf Seite 232.

Schritt 5: Konfigurieren des Access Gateways für die Kommunikation mit dem Access Gateway-Proxy

Beim Bereitstellen des Access Gateways in einer Double-Hop-DMZ müssen Sie das Access Gateway-Gerät in der ersten DMZ für die Kommunikation mit dem Access Gateway-Proxygerät in der zweiten DMZ konfigurieren.

Wenn Sie mehrere Geräte in der zweiten DMZ bereitgestellt haben, müssen Sie jedes Access Gateway in der ersten DMZ so konfigurieren, dass es mit jedem Access Gateway-Gerät in der zweiten DMZ Daten austauschen kann.

Mit der nachstehend beschriebenen Vorgehensweise können Sie die Kommunikation zwischen einem Access Gateway in der ersten DMZ und einem oder mehreren Access Gateway-Geräten in der zweiten DMZ konfigurieren.

So konfigurieren Sie das Access Gateway für die Kommunikation mit dem (den) Access Gateway-Proxygerät(en):

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway in der ersten DMZ.
2. Wählen Sie auf der Registerkarte **General Networking** unter **DMZ configuration** die Option **First hop in double DMZ**.
3. (Optional) Aktivieren Sie die Option **Configure for Advanced Access Control** nur, wenn Sie Access Gateway Advanced Edition bereitgestellt haben und eine Verbindung zu Advanced Access Control herstellen möchten.
4. Klicken Sie auf **Add**.
5. Geben Sie im Dialogfeld **Add appliance from second hop** Folgendes ein:

A. **FQDN or IP address:** Geben Sie den vollqualifizierten Domänennamen oder die IP-Adresse eines in der zweiten DMZ installierten Access Gateway-Proxygeräts ein.

B. **Port:** Der Standardport für eine SOCKS over SSL-Verbindung ist 443. Der Standardport für eine SOCKS-Verbindung ist 1080. Sie können die Standardports nach Bedarf ändern.

C. **Protocol:** Wählen Sie **SOCKS over SSL**, wenn Sie die SOCKS-Verbindung zum Access Gateway-Proxy in der zweiten DMZ mit SSL sichern möchten. Wählen Sie **SOCKS**, wenn Sie diese Verbindung ungesichert lassen möchten.

Hinweis: Wenn Sie die Option **SOCKS over SSL** aktivieren, müssen Sie die entsprechenden SSL-Zertifikate installieren. Weitere Informationen finden Sie unter „Schritt 9: Verwalten von SSL-Zertifikaten in einer Double-Hop-DMZ-Bereitstellung“ auf Seite 246.

D. (Optional) **Second hop appliance MAC address:** Füllen Sie dieses Feld nur aus, wenn Sie Access Gateway Advanced Edition bereitgestellt haben und eine Verbindung zu Advanced Access Control herstellen möchten. Diese Option wird nur angezeigt, wenn Sie **Configure for Advanced Access Control** in Schritt 3 aktiviert haben.

Geben Sie die MAC-Adresse der Netzwerkkarte für Schnittstelle 0 des in der zweiten DMZ installierten Access Gateway-Proxygeräts ein.

6. Klicken Sie auf die Schaltfläche **Validate**, um zu überprüfen, ob das Access Gateway in der ersten DMZ mit der angegebenen Adresse, dem angegebenen Protokoll und dem angegebenen Port eine Verbindung zum Access Gateway in der zweiten DMZ herstellen kann. Klicken Sie auf **OK**.
7. Wenn Sie mehrere Geräte in der zweiten DMZ installiert haben, wiederholen Sie Schritte 4 bis 6, bis jedes in der zweiten DMZ installierte Gerät in der Liste **Appliances in second hop** angezeigt wird.

Hinweis: Das Access Gateway in der ersten DMZ verwendet diese Liste für den Lastausgleich bei Verbindungen zu den in der zweiten DMZ installierten Geräten.

---

8. Klicken Sie auf **Submit**, um das Access Gateway neu zu starten.

Hinweis: Nähere Informationen zum Neustarten des Access Gateways finden Sie unter „Neustarten des Access Gateways“ auf Seite 48.

---

9. Wenn Sie mehrere Access Gateway-Geräte in der ersten DMZ installiert haben, wiederholen Sie alle o. g. Schritte für jedes Access Gateway in der ersten DMZ.

   Jedes in der ersten DMZ installierte Access Gateway muss für die Kommunikation mit allen in der zweiten DMZ installierten Access Gateway-Proxygeräten konfiguriert werden.

Schritt 6: Konfigurieren des Access Gateway-Proxys für die Kommunikation mit dem Access Gateway

Beim Bereitstellen von Access Gateway-Geräten in einer Double-Hop-DMZ-Konfiguration müssen Sie das Access Gateway in der zweiten DMZ für die Kommunikation mit dem Access Gateway in der ersten DMZ konfigurieren.

Führen Sie die nachstehend beschriebenen Schritte für jedes Gerät aus, das in der zweiten DMZ installiert ist.

So konfigurieren Sie das Access Gateway in der zweiten DMZ für die Kommunikation mit dem Access Gateway in der ersten DMZ:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway in der zweiten DMZ.
2. Wählen Sie auf der Registerkarte **General Networking** unter **DMZ configuration** die Option **Second hop in double DMZ**.
3. Wählen Sie unter **Protocol** entweder **SOCKS over SSL** oder **SOCKS** aus.

Wichtig: Das von Ihnen ausgewählte Protokoll muss mit dem Protokoll übereinstimmen, das Sie beim Konfigurieren des Access Gateways in der ersten DMZ ausgewählt haben.

---

4. Der Standardport unter **Port** ist entweder 443 (für sichere Verbindungen) oder 1080 (für unsichere Verbindungen). Der von Ihnen ausgewählte Port muss mit dem Port übereinstimmen, den Sie beim Konfigurieren des Access Gateways in der ersten DMZ ausgewählt haben.

5. (Optional) Dieser Schritt ist nur erforderlich, wenn Sie Access Gateway Advanced Edition bereitgestellt haben und eine Verbindung zu Advanced Access Control herstellen möchten.
   A. Aktivieren Sie die Option **Advanced Access Control**.
   B. Geben Sie im Feld **FQDN of first appliance in DMZ (required)** den vollqualifizierten Domänennamen des in der ersten DMZ installierten Geräts ein.
6. Klicken Sie auf **Submit**, um das Access Gateway neu zu starten.

Hinweis: Nähere Informationen zum Neustarten des Access Gateways finden Sie unter „Neustarten des Access Gateways“ auf Seite 48.

---

7. Wenn Sie mehrere Geräte in der zweiten DMZ installiert haben, wiederholen Sie diese Schritte für jedes Access Gateway in der zweiten DMZ.

Schritt 7: Konfigurieren des Access Gateways für den Secure Ticket Authority- und ICA-Datenverkehr

Wenn Sie das Access Gateway in einer Double-Hop-DMZ bereitstellen, müssen Sie das Access Gateway in der ersten DMZ für die Kommunikation mit dem Secure Ticket Authority- und ICA-Datenverkehr entsprechend konfigurieren.

- Konfigurieren Sie das Access Gateway in der ersten DMZ für die Kommunikation mit der Secure Ticket Authority, die im internen Netzwerk ausgeführt wird.
- (Optional) Erstellen Sie auf dem Access Gateway in der ersten DMZ eine ICA-Zugriffssteuerungsliste, um den Benutzerzugriff auf bestimmte Server zu beschränken, auf denen Presentation Server ausgeführt wird. Wenn Sie keine ICA-Zugriffssteuerungsliste erstellen, können Benutzer auf alle Server zugreifen, auf denen Presentation Server ausgeführt wird. Nähere Informationen zu ICA-Zugriffssteuerungslisten finden Sie unter „Konfigurieren der ICA-Zugriffssteuerung“ auf Seite 214.

So konfigurieren Sie das Access Gateway in der ersten DMZ für den Secure Ticket Authority- und ICA-Datenverkehr:

1. Klicken Sie auf die Registerkarte **Authentication** und anschließend auf die Registerkarte **Secure Ticket Authority**.
2. Geben Sie unter **Server running the STA** die IP-Adresse oder den vollqualifizierten Domänennamen des Servers ein, auf dem die Secure Ticket Authority installiert ist.
3. Geben Sie unter **STA path** den Pfad zur Secure Ticket Authority ein. Der Standardpfad lautet /Scripts/CtxSTA.dll.
4. Legen Sie unter **Connection type** fest, ob die Verbindung sicher (Secure) oder unsicher (Unsecure) ist.

   Hinweis: Nähere Informationen zu den für diese Verbindung verwendeten Ports und Zertifikaten finden Sie unter „Schritt 8: Öffnen der entsprechenden Ports in den Firewalls“ auf Seite 244 und „Schritt 9: Verwalten von SSL-Zertifikaten in einer Double-Hop-DMZ-Bereitstellung“ auf Seite 246.

   ---

5. Klicken Sie auf **Add**.

   Wenn die Secure Ticket Authority konfiguriert ist, werden der Server, der Pfad, die ID und der Verbindungstyp unter **Secure Ticket Authority Details** angezeigt.

   Hinweis: Sie können der Liste mehrere Server hinzufügen, auf denen die Secure Ticket Authority ausgeführt wird. Die Liste dieser Server sollte mit der Liste des Webinterface identisch sein.

Führen Sie diese Schritte nur aus, wenn Sie eine ICA-Zugriffssteuerungsliste erstellen möchten.

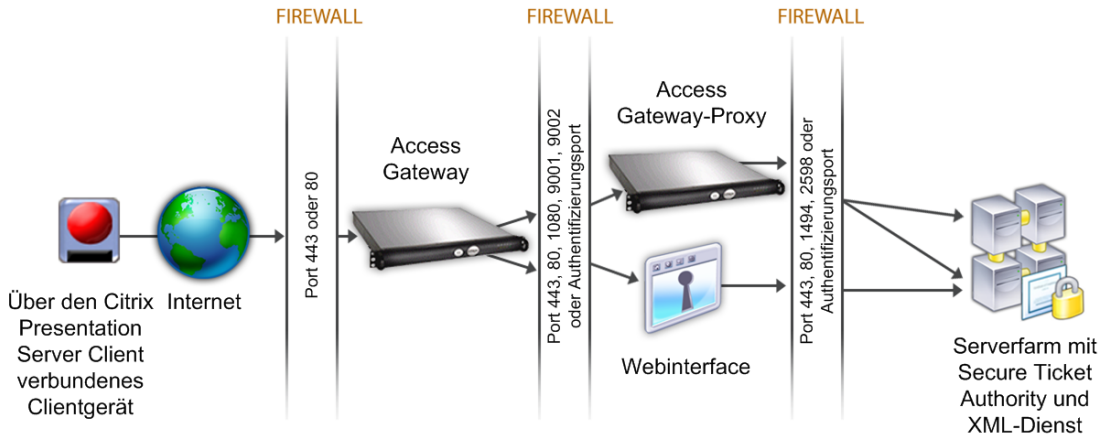
(Optional) So erstellen Sie eine ICA-Zugriffssteuerungsliste:

1. Klicken Sie auf die Registerkarte **Authentication** und dann auf die Registerkarte **ICA Access Control**.
2. Wenn Sie einen Bereich von Servern angeben möchten, auf denen Presentation Server ausgeführt wird, geben Sie in den Feldern **Starting IP address** und **Ending IP address** die erste und die letzte IP-Adresse ein.
3. Wählen Sie unter **Protocol** die Option **ICA** oder **CGP** (Citrix Gateway Protocol, das für Sitzungszuverlässigkeit und SmoothRoaming verwendet wird).
4. Behalten Sie die unter **Port** angegebene Standardportnummer bei oder geben Sie eine neue Nummer ein. Der Standardport für ICA-Verbindungen ist 1494. Der Standardport für die Sitzungszuverlässigkeit ist 2598. Klicken Sie auf **Add**.

Schritt 8: Öffnen der entsprechenden Ports in den Firewalls

Bei diesem Schritt müssen Sie gewährleisten, dass die entsprechenden Ports in den Firewalls offen sind, um die Verbindungen in einer Double-Hop-DMZ-Bereitstellung zu unterstützen.

Zwischen den verschiedenen Komponenten in einer Double-Hop-DMZ-Bereitstellung werden unterschiedliche Verbindungen hergestellt. Nähere Erläuterungen zum Verbindungsprozess finden Sie unter „Herstellen einer Clientverbindung in einer Double-Hop-DMZ“ auf Seite 250.



In dieser Abbildung sind die üblichen Ports dargestellt, die in einer Double-Hop-DMZ-Bereitstellung verwendet werden können. Anhand der Tabellen unten können Sie festlegen, welche Ports in den einzelnen Firewalls Ihrer Umgebung geöffnet werden sollen.

Die Tabelle zeigt, welche Verbindungen durch die erste Firewall hergestellt werden und welche Ports zur Unterstützung der Verbindungen offen sein müssen:

Verbindungen durch die erste Firewall	Verwendete Ports
Der Webbrowser stellt über das Internet eine Verbindung zum Access Gateway in der ersten DMZ her. Hinweis: Das Access Gateway enthält eine Option zum Weiterleiten von Verbindungen an Port 80 an einen sicheren Port. Wenn diese Option auf dem Access Gateway aktiviert ist, können Sie Port 80 an der ersten Firewall öffnen. Wenn ein Benutzer eine unverschlüsselte Verbindung zum Access Gateway an Port 80 herstellt, leitet das Access Gateway die Verbindung automatisch an einen sicheren Port weiter. Weitere Informationen finden Sie im Abschnitt „Umleiten von Verbindungen auf Port 80 an einen sicheren Port“ auf Seite 47.	Öffnen Sie TCP-Port 443 an der ersten Firewall. Sie können TCP-Port 80 öffnen, wenn die Option **Redirect any requests for port 80 to a secure port** auf dem Access Gateway aktiviert ist.
Der Presentation Server Client stellt über das Internet eine Verbindung zum Access Gateway in der ersten DMZ her.	Öffnen Sie TCP-Port 443 an der ersten Firewall.

Die Tabelle zeigt, welche Verbindungen durch die zweite Firewall hergestellt werden und welche Ports zur Unterstützung der Verbindungen offen sein müssen:

Verbindungen durch die zweite Firewall	Verwendete Ports
Das Access Gateway in der ersten DMZ stellt eine Verbindung zum Webinterface in der zweiten DMZ her.	Öffnen Sie entweder TCP-Port 80 für eine unsichere Verbindung oder TCP-Port 443 für eine sichere Verbindung durch die zweite Firewall.
Das Access Gateway in der ersten DMZ stellt eine Verbindung zum Access Gateway in der zweiten DMZ her.	Öffnen Sie entweder TCP-Port 1080 für eine unsichere SOCKS-Verbindung oder TCP-Port 443 für eine sichere SOCKS-Verbindung durch die zweite Firewall.
Wenn Sie die Anmeldeseitenauthentifizierung auf dem Access Gateway in der ersten DMZ aktiviert haben, muss dieses Access Gateway u. U. eine Verbindung zu einem Authentifizierungsserver im internen Netzwerk herstellen.	Öffnen Sie den TCP-Port, an dem der Authentifizierungsserver Verbindungen abhört, z. B. Port 1812 für RADIUS und Port 389 für LDAP.
Wenn Sie das Administration Tool auf einem Computer in der zweiten DMZ bereitgestellt haben, um Administratoraufgaben für Access Gateway-Geräte in der ersten DMZ auszuführen (wie unter „Planen der Installation des Access Gateway Administration Tools“ auf Seite 232 beschrieben), muss das Administration Tool eine Verbindung zum Access Gateway in der ersten DMZ herstellen.	Öffnen Sie TCP-Port 9002, damit das Administration Tool eine Verbindung zum Access Gateway herstellen kann. Öffnen Sie TCP-Port 9001, um über einen Webbrowser eine Verbindung zum Administration Portal auf dem Access Gateway herzustellen und das Administration Tool herunterzuladen und zu installieren.

Die Tabelle zeigt, welche Verbindungen durch die dritte Firewall hergestellt werden und welche Ports zur Unterstützung der Verbindungen offen sein müssen:

Verbindungen durch die dritte Firewall	Verwendete Ports
Das Webinterface in der zweiten DMZ stellt eine Verbindung zum XML-Dienst auf einem Computer im internen Netzwerk her, auf dem Presentation Server ausgeführt wird.	Für alle drei Verbindungen sind folgende Schritte erforderlich: Öffnen Sie entweder Port 80 für eine unsichere Verbindung oder Port 443 für eine sichere Verbindung durch die dritte Firewall.
Das Webinterface in der zweiten DMZ stellt eine Verbindung zur Secure Ticket Authority auf einem Computer im internen Netzwerk her, auf dem Presentation Server ausgeführt wird.	
Das Access Gateway in der zweiten DMZ stellt eine Verbindung zur Secure Ticket Authority im sicheren Netzwerk her.	
Das Access Gateway in der zweiten DMZ stellt eine ICA-Verbindung zu einer veröffentlichten Anwendung auf einem Computer im internen Netzwerk her, auf dem Presentation Server ausgeführt wird.	Öffnen Sie TCP-Port 1494, um ICA-Verbindungen durch die dritte Firewall zu unterstützen. Öffnen Sie TCP-Port 2598 anstelle von 1494, wenn Presentation Server Sitzungszuverlässigkeit unterstützt.
Wenn Sie die Anmeldeseitenauthentifizierung auf dem Access Gateway in der ersten DMZ aktiviert haben, muss dieses Access Gateway u. U. eine Verbindung zu einem Authentifizierungsserver im internen Netzwerk herstellen.	Öffnen Sie den TCP-Port, an dem der Authentifizierungsserver Verbindungen abhört, z. B. Port 1812 für RADIUS und Port 389 für LDAP.

Schritt 9: Verwalten von SSL-Zertifikaten in einer Double-Hop-DMZ-Bereitstellung

Bei diesem Schritt müssen Sie die SSL-Zertifikate installieren, die zum Sichern (Verschlüsseln) der Verbindungen zwischen den in einer Double-Hop-DMZ bereitgestellten Komponenten notwendig sind.

In einer Double-Hop-DMZ werden verschiedene Verbindungen zwischen den einzelnen bereitgestellten Komponenten hergestellt. Für diese Verbindungen gibt es keine durchgehende SSL-Verschlüsselung. Jede Verbindung kann jedoch einzeln verschlüsselt werden.

Zum Verschlüsseln einer Verbindung müssen Sie das entsprechende SSL-Zertifikat (entweder ein vertrauenswürdiges Stammzertifikat oder ein Serverzertifikat) auf den an der Verbindung beteiligten Komponenten installieren.

Die Tabelle zeigt, welche Verbindungen durch die erste Firewall hergestellt werden und welche SSL-Zertifikate zum Verschlüsseln der einzelnen Verbindungen erforderlich sind. Die Verschlüsselung der Verbindungen durch die erste Firewall ist zwingend erforderlich, um den über das Internet weitergeleiteten Datenverkehr zu schützen.

Verbindungen durch die erste Firewall	Für die Verschlüsselung erforderliche Zertifikate
Der Webbrowser stellt über das Internet eine Verbindung zum Access Gateway in der ersten DMZ her.	Auf dem Access Gateway in der ersten DMZ muss ein SSL-Serverzertifikat installiert sein. Auf dem Webbrowser muss ein Stammzertifikat installiert sein, das von der gleichen Zertifizierungsstelle signiert ist wie das Serverzertifikat auf dem Access Gateway.
Der Presentation Server Client stellt über das Internet eine Verbindung zum Access Gateway in der ersten DMZ her.	Das Zertifikat für diese Verbindung wird auf die gleiche Weise verwaltet wie die oben beschriebene Verbindung vom Webbrowser zum Access Gateway. Wenn Sie die Zertifikate zum Verschlüsseln der Webbrowser-Verbindung installiert haben, wird diese Verbindung auch mit diesen Zertifikaten verschlüsselt.

Die Tabelle zeigt, welche Verbindungen durch die zweite Firewall hergestellt werden und welche SSL-Zertifikate zum Verschlüsseln der einzelnen Verbindungen erforderlich sind. Die Verschlüsselung dieser Verbindungen erhöht die Sicherheit, ist jedoch nicht zwingend erforderlich.

Verbindungen durch die zweite Firewall	Für die Verschlüsselung erforderliche Zertifikate
Das Access Gateway in der ersten DMZ stellt eine Verbindung zum Webinterface in der zweiten DMZ her.	Auf dem Webinterface muss ein SSL-Serverzertifikat installiert sein. Auf dem Access Gateway in der ersten DMZ muss ein Stammzertifikat installiert sein, das von der gleichen Zertifizierungsstelle signiert ist wie das Serverzertifikat auf dem Webinterface.
Das Access Gateway in der ersten DMZ stellt eine Verbindung zum Access Gateway in der zweiten DMZ her.	Auf dem Access Gateway in der zweiten DMZ muss ein SSL-Serverzertifikat installiert sein. Auf dem Access Gateway in der ersten DMZ muss ein Stammzertifikat installiert sein, das von der gleichen Zertifizierungsstelle signiert ist wie das Serverzertifikat auf dem Access Gateway in der zweiten DMZ.

Die Tabelle zeigt, welche Verbindungen durch die dritte Firewall hergestellt werden und welche SSL-Zertifikate zum Verschlüsseln der einzelnen Verbindungen erforderlich sind. Die Verschlüsselung dieser Verbindungen erhöht die Sicherheit, ist jedoch nicht zwingend erforderlich.

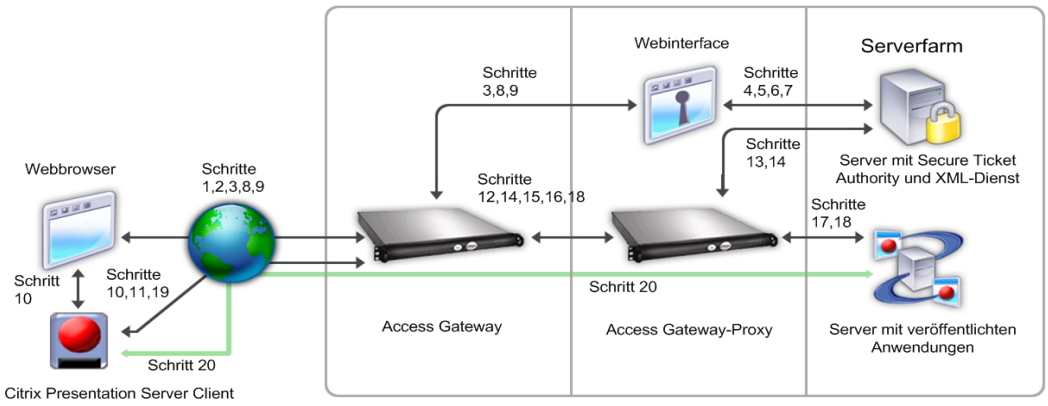
Verbindungen durch die dritte Firewall	**Für die Verschlüsselung erforderliche Zertifikate**
Das Webinterface in der zweiten DMZ stellt eine Verbindung zum XML-Dienst auf einem Presentation Server im internen Netzwerk her.	Wenn der XML-Dienst auf einem Microsoft IIS-Server (Internet Information Services) auf dem Presentation Server-Computer ausgeführt wird, muss ein SSL-Serverzertifikat auf dem IIS-Server installiert sein. Wenn der XML-Dienst ein Windows-Standarddienst ist (also sich nicht in IIS befindet), muss im SSL-Relay auf dem Computer, auf dem Citrix Presentation Server ausgeführt wird, ein SSL-Serverzertifikat installiert sein. Auf dem Webinterface muss ein Stammzertifikat installiert sein, das von der gleichen Zertifizierungsstelle signiert ist wie das Serverzertifikat, das auf dem Microsoft IIS-Server oder im SSL-Relay installiert ist.

Das Webinterface in der zweiten DMZ stellt eine Verbindung zur Secure Ticket Authority auf einem Computer im internen Netzwerk her, auf dem Citrix Presentation Server ausgeführt wird.	Das Zertifikat für diese Verbindung wird auf die gleiche Weise verwaltet wie die oben beschriebene Verbindung vom Webinterface zum XML-Dienst. Zum Verschlüsseln dieser Verbindung können Sie dieselben Zertifikate verwenden. (Das Serverzertifikat muss auf dem Microsoft IIS-Server oder im SSL-Relay installiert sein. Ein entsprechendes Stammzertifikat muss auf dem Webinterface installiert sein.)
Das Access Gateway in der zweiten DMZ stellt eine Verbindung zur Secure Ticket Authority auf einem Computer im internen Netzwerk her, auf dem Citrix Presentation Server ausgeführt wird.	Das SSL-Serverzertifikat für die Secure Ticket Authority wird bei dieser Verbindung auf die gleiche Weise verwaltet wie bei den beiden weiter oben in dieser Tabelle genannten Verbindungen. (Das Serverzertifikat muss auf dem Microsoft IIS-Server oder im SSL-Relay installiert sein. Auf dem Access Gateway in der zweiten DMZ muss ein Stammzertifikat installiert sein, das von der gleichen Zertifizierungsstelle signiert ist wie das Serverzertifikat, das von der Secure Ticket Authority und vom XML-Dienst verwendet wird.
Das Access Gateway in der zweiten DMZ stellt eine ICA-Verbindung zu einer veröffentlichten Anwendung auf einem Computer im internen Netzwerk her, auf dem Presentation Server ausgeführt wird.	Im SSL-Relay auf dem Computer, auf dem Citrix Presentation Server zum Hosten der veröffentlichten Anwendung ausgeführt wird, muss ein SSL-Serverzertifikat installiert sein. Auf dem Access Gateway-Proxy in der zweiten DMZ muss ein Stammzertifikat installiert sein, das von der gleichen Zertifizierungsstelle signiert ist wie das Serverzertifikat, das im SSL-Relay installiert ist.

Herstellen einer Clientverbindung in einer Double-Hop-DMZ

Dieser Abschnitt enthält eine detaillierte Beschreibung der einzelnen Schritte zur Herstellung von Clientverbindungen in einer Double-Hop-DMZ. Obwohl dieser Prozess kontinuierlich abläuft, wird er nachstehend zum besseren Verständnis in einzelne Phasen unterteilt. Es gibt vier Phasen:

- Clientauthentifizierung
- Erstellung von Sitzungstickets
- Starten des Clients
- Verbindungsherstellung



Diese Abbildung zeigt die einzelnen Schritte beim Herstellen von Clientverbindungen. Die in der Abbildung dargestellten Phasen entsprechen den Schritten, die in den Abschnitten „Clientauthentifizierung“, „Erstellung von Sitzungstickets“ und „Verbindungsherstellung“ unten erläutert werden. In einem sicheren Netzwerk führen Computer, auf denen Presentation Server ausgeführt wird, auch die Secure Ticket Authority, den XML-Dienst und veröffentlichte Anwendungen aus.

Clientauthentifizierung

Die Clientauthentifizierung läuft wie folgt ab:

1. Der Benutzer gibt in einem Webbrowser die Adresse des Access Gateways ein, z. B. https://www.ag.wxyco.com.
2. Die Verbindungsanforderung geht beim Access Gateway in der ersten DMZ ein.

3. Wenn auf dem Access Gateway Anmeldeseitenauthentifizierung aktiviert ist, leitet das Access Gateway die Access Gateway-Anmeldeseite an den Benutzer weiter. Nachdem der Benutzer seine Authentifizierungsinformationen auf der Anmeldeseite eingegeben hat, wird er vom Access Gateway authentifiziert. Dann leitet das Access Gateway die Anmeldeinformationen des Benutzers an das Webinterface weiter.

   Wenn die Anmeldeseitenauthentifizierung nicht aktiviert ist, nimmt das Access Gateway keine Authentifizierung vor. Das Access Gateway stellt eine Verbindung zum Webinterface her, ruft die Webinterface-Anmeldeseite auf und leitet die Webinterface-Anmeldeseite an den Benutzer weiter. Der Benutzer gibt seine Authentifizierungsinformationen auf der Webinterface-Anmeldeseite ein, die dann vom Access Gateway an das Webinterface zurückgeleitet werden.

4. Das Webinterface sendet die Anmeldeinformationen des Benutzers an den Citrix XML-Dienst, der in der Serverfarm im internen Netzwerk ausgeführt wird. Der Citrix XML-Dienst authentifiziert den Benutzer.

5. Der XML-Dienst erstellt eine Liste der veröffentlichten Anwendungen, auf die der Benutzer zugreifen darf, und leitet diese Liste an das Webinterface weiter.

Erstellung von Sitzungstickets

Die Erstellung von Sitzungstickets ist die zweite Phase beim Herstellen einer Clientverbindung in einer Double-Hop-DMZ-Bereitstellung.

6. Das Webinterface leitet für jede veröffentlichte Anwendung, auf die der Benutzer zugreifen darf, eine Anforderung für ein Sitzungsticket an die Secure Ticket Authority. Diese Anforderungen enthalten die IP-Adresse des Servers, der als Host für die veröffentlichte Anwendung fungiert.

7. Die Secure Ticket Authority speichert die IP-Adressen der Server, die als Host für die veröffentlichten Anwendungen fungieren. Dann leitet die Secure Ticket Authority die angeforderten Sitzungstickets an das Webinterface weiter.

   Jedes Sitzungsticket enthält nicht die tatsächliche IP-Adresse, sondern ein Alias, das die IP-Adresse des Servers darstellt, der als Host für die veröffentlichte Anwendung fungiert.

8. Das Webinterface erstellt eine ICA-Datei für jede veröffentlichte Anwendung. Die ICA-Datei enthält das von der Secure Ticket Authority ausgestellte Ticket.

   Im Webinterface wird daraufhin eine Webseite mit einer Liste der Links zu den veröffentlichten Anwendungen (ICA-Dateien) angezeigt, die an den Clientwebbrowser weitergeleitet wird.

Starten des Clients

Das Starten des Clients ist die dritte Phase beim Herstellen einer Clientverbindung in einer Double-Hop-DMZ-Bereitstellung.

9. Der Benutzer klickt auf der vom Webinterface bereitgestellten Webseite auf einen Link zu einer veröffentlichten Anwendung. Das Webinterface leitet die ICA-Datei für diese veröffentlichte Anwendung an den Clientbrowser weiter.

   Durch die in der ICA-Datei enthaltenen Daten wird der Webbrowser angewiesen, einen Citrix Presentation Server Client zu starten.

   Die ICA-Datei enthält auch den vollqualifizierten Domänennamen oder den DNS-Namen des Access Gateways in der ersten DMZ.

10. Der Webbrowser startet den Presentation Server Client, der mit dem in der ICA-Datei enthaltenen Access Gateway-Namen eine Verbindung zum Access Gateway in der ersten DMZ herstellt.

    Es kommt zum ersten SSL/TLS-Handshake, um die Identität des Servers zu ermitteln, auf dem das Access Gateway ausgeführt wird.

Verbindungsherstellung

Die endgültige Herstellung der Verbindung ist die vierte und letzte Phase beim Herstellen einer Clientverbindung in einer Double-Hop-DMZ-Bereitstellung.

11. Der Presentation Server Client leitet das Secure Ticket Authority-Ticket für die veröffentlichte Anwendung an das Access Gateway in der ersten DMZ weiter.

12. Das Access Gateway in der ersten DMZ stellt eine Verbindung zur Secure Ticket Authority im internen Netzwerk, um das Ticket zu überprüfen.

    Zu diesem Zweck stellt das Access Gateway eine SOCKS-Verbindung oder eine SOCKS over SSL-Verbindung zum Access Gateway-Proxy in der zweiten DMZ her.

13. Der Access Gateway-Proxy in der zweiten DMZ leitet die Anforderung zur Ticketüberprüfung an die Secure Ticket Authority im internen Netzwerk weiter.

    Die Secure Ticket Authority überprüft das Ticket und ordnet es dem Computer zu, auf dem Citrix Presentation Server als Host für die veröffentlichte Anwendung ausgeführt wird.

14. Die Secure Ticket Authority sendet eine Antwort an den Access Gateway-Proxy in der zweiten DMZ, die an das Access Gateway in der ersten DMZ weitergeleitet wird.

    Diese Antwort schließt die Ticketüberprüfung ab und enthält die IP-Adresse des Computers, auf dem Citrix Presentation Server als Host für die veröffentlichte Anwendung ausgeführt wird.

15. Das Access Gateway in der ersten DMZ prüft die IP-Adresse des Citrix Presentation Server-Computers anhand der ICA-Zugriffssteuerungsliste (sofern vorhanden), um sicherzustellen, dass Benutzer auf den Citrix Presentation Server-Computer zugreifen dürfen.

16. Das Access Gateway in der ersten DMZ schließt die Adresse des Computers, auf dem Citrix Presentation Server ausgeführt wird, in das Clientverbindungspaket ein und leitet dieses Paket an den Access Gateway-Proxy in der zweiten DMZ weiter.

17. Der Access Gateway-Proxy in der zweiten DMZ erstellt eine Verbindungsanforderung an den im Verbindungspaket angegebenen Computer, auf dem Citrix Presentation Server ausgeführt wird.

18. Dieser Computer sendet eine Antwort an den Access Gateway-Proxy in der zweiten DMZ. Der Access Gateway-Proxy in der zweiten DMZ leitet diese Antwort an das Access Gateway in der ersten DMZ weiter, um die Verbindung zwischen dem Computer, auf dem Citrix Presentation Server ausgeführt wird, und dem Access Gateway in der ersten DMZ herzustellen.

19. Das Access Gateway in der ersten DMZ schließt den SSL/TLS-Handshake mit dem Presentation Server Client durch Weiterleitung des endgültigen Verbindungspakets an den Client ab. Dadurch ist die Verbindung vom Presentation Server Client zu Citrix Presentation Server hergestellt.

20. Jetzt können Daten zwischen dem Presentation Server Client und dem Computer, auf dem Citrix Presentation Server ausgeführt wird, über das Access Gateway in der ersten DMZ und den Access Gateway-Proxy in der zweiten DMZ übertragen werden.

KAPITEL 12

Warten des Access Gateways

In diesem Kapitel werden die Wartungseinstellungen für das Access Gateway und die Tools, mit denen sie konfiguriert werden, beschrieben.

Hinweis: Alle Konfigurationsänderungen werden automatisch übernommen und führen für die mit dem Access Gateway verbundenen Benutzer zu keinerlei Betriebsunterbrechungen. Richtlinienänderungen treten sofort in Kraft. Wenn eine Verbindung gegen eine neue Richtlinie verstößt, wird sie geschlossen.

In diesem Kapitel werden die folgenden Themen behandelt:

- Access Gateway-Verwaltungstools
- Aktualisieren der Access Gateway-Software
- Neuinstallieren der Access Gateway-Software
- Speichern und Wiederherstellen der Access Gateway-Konfiguration
- Neustarten und Herunterfahren des Access Gateways
- Zulassen von ICMP-Verkehr
- Konfigurieren persönlicher Firewalls von Drittanbietern

Access Gateway-Verwaltungstools

Bei der Access Gateway-Verwaltung wird eine Kombination aus einem Webseitenportal, dem Administration Tool und Tools zur Überwachung von Netzwerkverbindungen verwendet. Das Administration Tool enthält sämtliche Steuerelemente für die Access Gateway-Konfiguration. Nur die Verwaltung des Administratorkontos kann ausschließlich über das Administration Portal und die serielle Konsole vorgenommen werden. Folgende Verwaltungstools stehen zur Verfügung:

- Das Administration Tool enthält Konfigurationssteuerelemente für das Gerät.
- Im Administration Portal finden Sie Downloads und Sie können einige Access Gateway-Einstellungen verwalten.
- Der Administration Desktop bietet Überwachungstools für das Access Gateway.

Administration Tool

Mit dem Administration Tool können Sie globale Einstellungen konfigurieren und diese dann auf die verschiedenen Access Gateway-Geräte im Netzwerk übertragen.

Im linken Bereich des Administration Tool-Fensters finden Sie Hilfeinformationen für die aktuell ausgewählte Registerkarte. Die Onlinehilfe passt sich an die Aufgabe an, die Sie gerade ausführen.

Außerdem werden im Bereich **Alerts** über der Onlinehilfe Warnungen angezeigt. Warnungen informieren Sie, wenn auf dem Access Gateway ein Problem aufgetreten ist, z. B. eine fehlende Lizenz oder ein Zertifikat.

Das Administration Tool wird vom Administration Portal aus heruntergeladen und installiert.

Wichtig: Wenn Sie ein Upgrade von einer älteren Access Gateway-Version vornehmen, müssen Sie das Administration Tool zunächst über das Dialogfeld **Software** in der Systemsteuerung deinstallieren, bevor Sie die neueste Version vom Administration Portal herunterladen und installieren.

So installieren und starten Sie das Administration Tool:

1. Klicken Sie im Administration Portal auf **Downloads**.
2. Klicken Sie unter **Access Gateway Administration Tool** auf **Install the Access Gateway Administration Tool**. Klicken Sie auf **Öffnen**.

3. Folgen Sie den Anweisungen im Installationsassistenten, um das Administration Tool zu installieren.
4. Klicken Sie zum Starten des Administration Tools auf **Start > Programme > Citrix > Access Gateway Administration Tool 4.5 > Access Gateway Administration Tool 4.5** oder klicken Sie auf das Symbol auf dem Desktop.
5. Geben Sie im Dialogfeld **Administrator Login** unter **Host (IP or FQDN)** die IP-Adresse des Access Gateways ein.
6. Geben Sie im Feld **Administrator Username** als Benutzernamen **root** ein.
7. Geben Sie im Feld **Administrator Password** das Standardkennwort **rootadmin** oder das neue Kennwort ein, wenn es mit der seriellen Konsole oder dem Administration Portal geändert wurde.

Installieren mehrerer Versionen des Administration Tools

Wenn Sie in Ihrem Netzwerk mehrere Geräte haben und es sich dabei um verschiedene Versionen handelt, können Sie mehrere Instanzen des Administration Tools auf Ihrem Computer installieren. Der Grund hierfür ist , dass frühere Versionen des Administration Tools nicht mit dieser Access Gateway-Version verwendet werden können. Mit dem Administration Tool dieser Version können außerdem frühere Versionen des Access Gateways nicht verwaltet werden. Auf der Registerkarte **Access Gateway Cluster** können Sie auf der Registerkarte **Statistics** herausfinden, welche Version des Tools Sie verwenden.

Administration Portal

Das Administration Portal bietet eine webbasierte Benutzeroberfläche für Administratoren. Es verfügt über mehrere Registerkarten, die Ihnen die Verwaltung des Access Gateways erleichtern sollen.

So öffnen Sie das Administration Portal:

1. Geben Sie in einem Webbrowser https://***AccessGatewayFQDN*:9001/** ein.
2. Geben Sie den Administratorbenutzernamen und das Kennwort ein. Die Standardwerte lauten **root** und **rootadmin**.

   Das Administration Portal wird geöffnet. Nachfolgend werden die Tasks beschrieben, die Sie mit dem Administration Portal ausführen können.

Herunterladen von Tools und Dokumentation

Auf der Seite **Downloads** haben Sie folgende Optionen:

- Herunterladen des Administration Tools
- Herunterladen und Installieren oder Starten des Administration Desktops
- Herunterladen der Access Gateway-Dokumentation
- Herunterladen der Portalseitenvorlagen
- Herunterladen der Muster-E-Mail für Benutzer

Konfigurieren des Administratorkennworts

Das Access Gateway verfügt über ein standardmäßiges Administratorkonto mit uneingeschränktem Zugriff auf das Gerät. Um das Access Gateway vor unbefugtem Zugriff zu schützen, sollten Sie das Standardkennwort während der Erstkonfiguration ändern. Der Standardbenutzername für den Access Gateway-Administrator lautet **root** und das zugehörige Kennwort **rootadmin**. Das Administratorkennwort kann im Administration Portal oder der seriellen Konsole geändert werden. Citrix empfiehlt, dass Sie das Administratorkennwort mit der seriellen Konsole nach der Installation des Geräts ändern. Weitere Informationen hierzu finden Sie unter „Konfigurieren der TCP/IP-Einstellungen mit dem seriellen Kabel“ auf Seite 42.

Hinweis: Wenn Sie das Standardkennwort für das Administratorkonto auf den Standardwert zurücksetzen möchten, müssen Sie die Access Gateway-Serversoftware neu installieren.

Das neue Kennwort darf bis zu 127 Zeichen enthalten. Weder am Anfang noch am Ende darf ein Leerzeichen stehen.

So ändern Sie das Administratorkennwort im Administration Portal:

1. Klicken Sie im Administration Portal auf der Registerkarte **Administration** auf **Admin Password**.
2. Geben Sie unter **Administrator Password** das neue Kennwort ein.
3. Klicken Sie auf **Change Password**.

Anzeigen von Protokollinformationen

Auf der Seite **Logging** wird das Protokoll für das Access Gateway angezeigt. Die hier angezeigten Informationen sind mit denen identisch, die im Administration Tool auf der Registerkarte **Access Gateway Cluster > Logging/Settings** angezeigt werden.

Ausführen von Wartungsaufgaben

Auf der Seite **Maintenance** können Sie Verwaltungsaufgaben ausführen. Dazu gehören folgende Aufgaben:

- Hochladen signierter Zertifikate (.crt)
- Hochladen privater Schlüssel und Zertifikate (.pem)
- Eingeben des Kennworts für einen privaten Schlüssel
- Hochladen gespeicherter Konfigurationen oder Upgrades
- Suchen nach Geräteaktualisierungen
- Speichern der Gerätekonfiguration
- Neustarten und Herunterfahren des Geräts
- Initialisieren des Geräts

Durch Klicken auf **Log Out** können Sie sich vom Administration Portal abmelden.

Verwalten externer Verbindungen mit dem Administration Portal

Wenn Sie das Access Gateway so konfigurieren, dass beide Netzwerkadapter verwendet werden, kann der externe Adapter standardmäßig für den Zugriff auf das Administration Portal vom Internet aus verwendet werden. Sie können den Zugriff vom Internet auf das Administration Portal blockieren, indem Sie die Option **Enable external administration** deaktivieren.

So blockieren Sie den externen Zugriff auf das Administration Portal:

1. Klicken Sie im Administration Tool auf die Registerkarte **Access Gateway Cluster** und öffnen Sie das Fenster für das Access Gateway.
2. Deaktivieren Sie auf der Registerkarte **Administration** unter **Access management** die Option **Enable external administration**.
3. Klicken Sie auf **Apply Change**.

Überwachen des Access Gateways mit dem Administration Desktop

Der Administration Desktop ermöglicht den Zugriff auf die Access Gateway-Überwachungstools. Über die Taskleiste erhalten Sie mit nur einem Mausklick Zugriff auf eine Vielzahl von Standardüberwachungsanwendungen für Linux sowie auf das Tool Citrix Real-time Monitor für die Anzeige und Verwaltung der offenen Verbindungen und die Einstellung der Systemzeit.

In der Mitte der Taskleiste befinden sich Schaltflächen zum Wechseln zu einem anderen Arbeitsbereich und Taskleistenschaltflächen. Die rechte Seite der Taskleiste enthält Informationen zur Prozessor- und Netzwerknutzung und zeigt die Systemzeit an.

Der Administration Desktop wird vom Administration Portal aus geöffnet.

So laden Sie den Administration Desktop herunter und öffnen ihn:

1. Führen Sie im Administration Portal auf der Registerkarte **Downloads** unter **Access Gateway Administration Desktop** einen der folgenden Schritte aus:
   - Klicken Sie zum Starten des Administration Desktops auf **Launch the Access Gateway Administrative Desktop** und dann auf **Ausführen**.
   - Klicken Sie zum Installieren des Administration Desktops auf **Install the Access Gateway Administration Desktop** und dann auf **Ausführen**.
2. Geben Sie im Dialogfeld **Citrix Access Gateway Remote Admin Desktop** Ihren Benutzernamen und das Kennwort ein.
3. Klicken Sie auf **Connect**.

Hinweis: Wenn Sie das Access Gateway so konfigurieren, dass beide Netzwerkadapter verwendet werden, steht das Administration Portal von beiden Adaptern aus zur Verfügung. Wenn Sie den Administratorzugriff über den Netzwerkadapter verhindern möchten, der eine externe Verbindung aufbaut, finden Sie Informationen dazu unter „Verwalten externer Verbindungen mit dem Administration Portal“ auf Seite 259.

Aktualisieren der Access Gateway-Software

Die Software auf dem Access Gateway kann bei Veröffentlichung neuer Releases über ein Upgrade aktualisiert werden. Ob neue Aktualisierungen zur Verfügung stehen, erfahren Sie im Administration Portal. Ein Upgrade auf ein neues Release ist nur dann möglich, wenn Ihre Access Gateway-Lizenzen zum Zeitpunkt der Veröffentlichung der Aktualisierung am Subscription Advantage-Programm teilnehmen. Das Subscription Advantage-Abonnement kann jederzeit erneuert werden. Weitere Informationen finden Sie auf der Citrix Support-Website unter http://www.citrix.com.

So prüfen Sie, ob neue Softwareaktualisierungen veröffentlicht wurden:

1. Öffnen Sie das Administration Portal und klicken Sie auf **Maintenance**.
2. Klicken Sie auf **Check for Server Upgrade**.

   Die Citrix Support-Website wird geöffnet und Sie können, so vorhanden, das Upgrade von der Website herunterladen.

Mit dieser Access Gateway-Version können gespeicherte Konfigurationen früherer Versionen des Geräts gelesen werden. Wenn eine gespeicherte Konfiguration einer früheren Version mit Access Gateway Version 4.5 wiederhergestellt wird, wird sie automatisch in das neue Format konvertiert. Wenn Sie ein Upgrade von einer älteren Version des Access Gateways auf diese Version durchführen, ist es wichtig, die aktuelle Konfiguration vorher zu speichern. Wenn Sie eine frühere Version der Software wiederherstellen müssen, muss das Gerät komplett neu erstellt werden. Nach der Neuerstellung des Geräts können Sie die gespeicherte Konfiguration wiederherstellen.

Wichtig: Das Access Gateway hat das Standardadministratorkennwort *rootadmin*. Wenn Sie das Kennwort auf ein Kennwort mit weniger als sechs Zeichen ändern, werden nach dem Upgrade des Geräts auf Version 4.5 Verbindungen zum Administration Tool und Administration Portal abgelehnt. Stellen Sie vor dem Upgrade des Geräts sicher, dass das Administratorkennwort mindestens sechs Zeichen enthält.

Wiederherstellen gespeicherter privater Zertifikatschlüssel

Die privaten Schlüssel von vom Access Gateway Version 4.5 erstellten Zertifikaten sind jetzt verschlüsselt und durch Kennwörter geschützt. Die neuen privaten Schlüssel sind nicht mit früheren Versionen der Access Gateway-Software kompatibel. Aus diesem Grund ist es wichtig, vor einem Upgrade die aktuelle Konfiguration zu speichern.

Wenn eine gespeicherte Konfiguration auf dem Gerät wiederhergestellt wird, ist das Kennwort für den privaten Schlüssel nicht erforderlich. Das Kennwort wird auch beim Speichern der Gerätkonfiguration nicht benötigt. Das Kennwort ist beim Installieren oder Erstellen eines Zertifikats mit Access Gateway Version 4.5 erforderlich. Wenn Sie ein neues, mit Version 4.5 erstelltes Zertifikat hochladen oder eine gespeicherte Konfiguration einer früheren Version der Software wiederherstellen, werden Sie zur Eingabe des Kennworts aufgefordert. Wenn der private Schlüssel des Zertifikats verschlüsselt ist, kann der Schlüssel mit dem Kennwort entschlüsselt werden. Wenn der private Schlüssel nicht verschlüsselt ist, wird er mit dem Kennwort verschlüsselt. Wenn Sie ein Upgrade von einer früheren Version des Access Gateways durchführen und der private Schlüssel kein Kennwort hat, wird ein zufällig erstelltes Kennwort zugewiesen und der private Schlüssel wird damit verschlüsselt.

Achtung: Wenn Sie die Konfiguration unter Version 4.5 des Access Gateways speichern, installieren Sie diese Konfiguration nicht auf früheren Versionen des Geräts. Der Grund hierfür ist, dass der private Schlüssel in Version 4.5 verschlüsselt ist und ältere Versionen ihn nicht entschlüsseln können. Dadurch wird das Gerät funktionsuntüchtig.

Installieren des Software-Upgrades

Zum Hochladen der neuen Software auf das Gerät steht Ihnen das Administration Tool zur Verfügung. Lesen Sie sich vor der Installation des Upgrades die Dokumentation zur Software durch.

Hinweis: Wenn Sie ein Serverupgrade hochladen, beendet das Access Gateway alle aktiven Sitzungen. Es empfiehlt sich daher, Upgrades möglichst dann durchzuführen, wenn der Netzwerkverkehr eher gering ist.

So laden Sie ein Upgrade auf das Access Gateway hoch:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf die Registerkarte **Administration**.
3. Klicken Sie neben **Upload an upgrade or saved configuration** auf **Browse**.

4. Suchen Sie die Upgradedatei, die hochgeladen werden soll, und klicken Sie auf **Öffnen**.

   Die Datei wird hochgeladen und Sie werden zum Neustart des Access Gateways aufgefordert.

Hinweis: Sie können die Access Gateway-Software auch über die Seite **Maintenance** im Administration Portal aktualisieren.

Wenn Sie das Access Gateway aktualisieren, werden alle Ihre Konfigurationseinstellungen gespeichert. Informationen zum Speichern und Wiederherstellen einer Konfiguration finden Sie unter „Speichern und Wiederherstellen der Access Gateway-Konfiguration“ auf Seite 264.

Neuinstallieren der Access Gateway-Software

Wenn Sie die Access Gateway-Serversoftware neu installieren müssen, verwenden Sie die mit dem Gerät gelieferte CD-ROM.

So installieren Sie die Access Gateway-Serversoftware neu:

1. Speichern Sie die Access Gateway-Konfigurationseinstellungen wie unter „Speichern und Wiederherstellen der Access Gateway-Konfiguration“ auf Seite 264 beschrieben.
2. Stellen Sie sicher, dass das Access Gateway mit einem Computer verbunden ist, auf dem die Terminalemulationssoftware ausgeführt werden kann. Schalten Sie beide Systeme ein.
3. Legen Sie die Access Gateway-Wiederherstellungs-CD-ROM in das CD-Laufwerk des Access Gateways ein, um das Installationsprogramm zu starten.

   Wenn die Installation abgeschlossen ist, zeigt die serielle Konsole eine entsprechende Meldung an.
4. Nehmen Sie die Wiederherstellungs-CD-ROM wieder heraus und schalten Sie das Access Gateway aus.
5. Schalten Sie das Access Gateway ein.
6. Stellen Sie die Konfigurationseinstellungen wieder her. Informationen hierzu finden Sie unter „Speichern und Wiederherstellen der Access Gateway-Konfiguration“ auf Seite 264.

Speichern und Wiederherstellen der Access Gateway-Konfiguration

Wenn Sie das Access Gateway aktualisieren, werden alle Ihre Konfigurationseinstellungen, einschließlich der hochgeladenen Zertifikate, Lizenzen und Portalseiten, automatisch wiederhergestellt. Wenn Sie die Access Gateway-Software jedoch neu installieren, müssen Sie Ihre Konfigurationseinstellungen manuell speichern und dann wiederherstellen.

Hinweis: Zum Speichern und Wiederherstellen der Konfigurationseinstellungen steht Ihnen auch die Registerkarte **Maintenance** des Administration Portals zur Verfügung.

So speichern Sie die Access Gateway-Konfiguration:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** im Bereich **Upgrade and configuration management** neben **Save the current configuration** auf **Save Configuration**.
3. Speichern Sie die Datei **config.restore** auf Ihrem Computer.

Daraufhin wird die gesamte Access Gateway-Konfiguration gespeichert, einschließlich der Systemdateien, installierten Lizenzen und installierten Serverzertifikate.

Nach der Installation der Access Gateway-Software können Sie die gespeicherte Konfiguration wiederherstellen.

So stellen Sie eine gespeicherte Konfiguration wieder her:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** im Bereich **Upgrade and configuration management** neben **Upload an upgrade or saved configuration** auf **Browse**.
3. Suchen Sie die Datei config.restore und klicken Sie auf **Öffnen**.

   Nachdem die Konfigurationsdatei hochgeladen wurde, starten Sie das Access Gateway neu und alle Konfigurationseinstellungen, Lizenzen und Zertifikate werden wiederhergestellt.

Wenn Sie die RSA SecurID-Authentifizierung verwenden, müssen Sie das Node Secret auf dem RSA ACE/Server zurücksetzen (siehe dazu „Zurücksetzen des Node Secret“ auf Seite 103). Da die Access Gateway-Einstellungen wiederhergestellt wurden, befindet sich das Node Secret nicht mehr auf dem Access Gateway, sodass jeder Versuch einer RSA ACE/Server-Authentifizierung scheitert, bis das Node Secret zurückgesetzt worden ist.

Neustarten und Herunterfahren des Access Gateways

Sie können das Access Gateway mit dem Administration Portal oder dem Administration Tool neu starten.

Neustarten des Access Gateways

Wenn Sie Änderungen am Access Gateway vorgenommen haben, müssen Sie das Gerät u. U. neu starten.

So starten Sie das Access Gateway neu:

1. Klicken Sie im Administration Tool auf die Registerkarte **Access Gateway Cluster** und öffnen Sie das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** im Bereich **Access Gateway management** neben **Restart the appliance** auf **Restart**.

   - oder -

   Klicken Sie im Menü **Action** auf **Restart** ***Access Gateway-Name***, wobei *Access Gateway-Name* der Name des Geräts ist.

Sie können das Access Gateway auch über das Administration Portal neu starten.

So starten Sie das Access Gateway über das Administration Portal neu:

Klicken Sie auf der Registerkarte **Maintenance** neben **Restart the server** auf **Restart**.

Herunterfahren des Access Gateways

Fahren Sie das Access Gateway niemals herunter, indem Sie den Netzschalter drücken. Verwenden Sie die Befehle im Administration Tool oder im Administration Portal zum Herunterfahren des Geräts. Der Netzschalter darf nur zum Einschalten des Geräts verwendet werden.

So fahren Sie das Access Gateway herunter:

1. Klicken Sie im Administration Tool auf die Registerkarte **Access Gateway Cluster** und öffnen Sie das Fenster für das Access Gateway.
2. Klicken Sie auf der Registerkarte **Administration** im Bereich **Access Gateway management** neben **Shut down the appliance** auf **Shut down**.

   - oder -

   Klicken Sie im Menü **Action** auf **Shut down** ***Access Gateway-Name***, wobei *Access Gateway-Name* der Name des Geräts ist.

Das Access Gateway kann auch mit dem Administration Portal heruntergefahren werden.

So fahren Sie das Access Gateway über das Administration Portal herunter:

Klicken Sie auf der Registerkarte **Maintenance** neben **Shut down the server** auf **Shut down**.

Initialisieren des Access Gateways

Nach dem Ändern der Verwaltungseinstellungen müssen Sie das Access Gateway initialisieren, damit die Änderungen wirksam werden. Wenn die Initialisierung des Access Gateways erforderlich ist, wird im Administration Tool im Bereich **Alerts** eine Meldung angezeigt.

Beim Initialisieren des Access Gateways werden alle Benutzer vom Access Gateway getrennt. Sie sollten die Initialisierung daher zu Zeiten durchführen, wenn möglichst wenige Benutzer mit dem Access Gateway verbunden sind.

So initialisieren Sie das Access Gateway:

Klicken Sie auf der Registerkarte **Administration** neben **Initialize the appliance** auf **Initialize**.

Zulassen von ICMP-Verkehr

ICMP-Verkehr (Internet Control Message Protocol) zum Access Gateway ist standardmäßig deaktiviert. Wenn Sie ICMP-Verkehr zulassen möchten, verwenden Sie die Registerkarte **Access Gateway Cluster > Administration**.

Wenn ICMP-Verkehr zugelassen ist, können die Benutzer Server im internen, sicheren Netzwerk „pingen“. Das Access Gateway selbst kann keinen ICMP-Verkehr empfangen.

So lassen Sie ICMP-Verkehr zu:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Aktivieren Sie auf der Registerkarte **Administration** im Bereich **Access management** die Option **Allow ICMP traffic**.
3. Klicken Sie auf **Apply Change**.

Konfigurieren persönlicher Firewalls von Drittanbietern

Wenn ein Benutzer keine Verbindung zum Access Gateway herstellen oder nicht auf zugelassene Ressourcen zugreifen kann, wird der Verkehr möglicherweise durch die Firewallsoftware auf dem Computer des Benutzers blockiert. Das Access Gateway kann zusammen mit allen persönlichen Firewalls eingesetzt werden, sofern die Anwendung die Festlegung eines vertrauenswürdigen Netzwerks oder einer IP-Adresse für das Access Gateway ermöglicht.

Citrix empfiehlt, dass die persönliche Firewall des Benutzers dem Secure Access Client vollen Zugriff gewähren sollte. Wenn Sie keinen vollständigen Zugriff gewähren möchten, sollten die folgenden UDP- und UDP/TCP-Ports offen sein:

- 10000 (UDP)
- 10010 (UDP/TCP)
- 10020 (UDP)
- 10030 (UDP)

Persönliche Firewalls müssen so konfiguriert sein, dass sie eingehenden und ausgehenden Datenverkehr von der IP-Adresse des Access Gateways oder dem vollqualifizierten Domänennamen zulassen. Auf der Seite **Eigenschaften** im Secure Access Client können Sie sehen, welche Ports offen sind. Sie öffnen die Seite über das Verbindungssymbol im Infobereich. Die offenen Ports werden auf der Registerkarte **Details** aufgeführt.

So zeigen Sie die Secure Access Client-Statuseigenschaften an:

Doppelklicken Sie im Infobereich auf das Secure Access Client-Verbindungssymbol. Sie können stattdessen auch mit der rechten Maustaste auf das Symbol klicken und im Kontextmenü den Befehl **Eigenschaften** wählen.

Das Dialogfeld **Citrix Secure Access Client** wird angezeigt.

Die Verbindungseigenschaften enthalten nützliche Informationen für die Problembehandlung. Hierzu gehören z. B. folgende Eigenschaften:

- Die Registerkarte **Allgemein** enthält Verbindungsinformationen.
- Auf der Registerkarte **Details** finden Sie Serverinformationen und eine Liste der gesicherten Netzwerke, auf die der Client zugreifen kann.
- Die Registerkarte **Zugriffslisten** enthält die Zugriffssteuerungslisten (ACLs), die für die Benutzerverbindung konfiguriert sind. Diese Registerkarte wird nur für Benutzer angezeigt, die Mitglied einer Gruppe sind. Wenn für eine Gruppe keine Zugriffssteuerungsliste konfiguriert ist, wird die Registerkarte auch nicht angezeigt.

Im Folgenden finden Sie Vorschläge für Firewalls, die häufig mit dem Access Gateway eingesetzt werden.

Hinweis: Vollständige Anweisungen zur Konfiguration der Firewalls finden Sie in der Herstellerdokumentation.

BlackICE PC Protection

Damit der Secure Access Client eine Verbindung zum Internet und zu den vom Access Gateway zugelassenen Ressourcen herstellen kann, sollten Sie den Schutzgrad auf einen Wert unter „Paranoid“ einstellen, da dies die Ausführung von Anwendungen verhindern würde. Fügen Sie außerdem die IP-Adresse des Access Gateways als vertrauenswürdige Zone hinzu. Sie müssen auch die IP-Adresse oder den IP-Adressbereich der zugelassenen Ressourcen als vertrauenswürdige Zonen hinzufügen.

McAfee Personal Firewall Plus

Mit den McAfee Personal Firewall Plus-Einstellungen kann der Secure Access Client eine Verbindung zum Internet und den vom Access Gateway zugelassenen Ressourcen herstellen.

Bei den Einstellungen wird davon ausgegangen, dass als Sicherheitsstufe die Einstellung **Standardsicherheit** ausgewählt ist. Stellen Sie sicher, dass die IP-Adresse oder der IP-Adressbereich der zugelassenen Ressourcen als vertrauenswürdige IP-Adressen hinzugefügt wurden. Wählen Sie in der Liste **Systemdienste** alle Dienste aus, die über die VPN-Verbindung verwendet werden sollen..

Hinweis: Wenn der Secure Access Client installiert ist, werden Sie standardmäßig von Personal Firewall Plus aufgefordert, den Zugriff für diese Anwendung zu gewähren oder zu sperren. Wählen Sie **Zugriff gewähren**.

Norton Personal Firewall

Bei Verwendung der Norton Personal Firewall-Standardeinstellungen können Sie einfach auf die Warnmeldungen der Programmsteuerung reagieren, wenn Sie das erste Mal versuchen, den Secure Access Client zu starten, oder wenn Sie auf einen gesperrten Speicherort oder eine gesperrte Anwendung zugreifen. Wenn Sie auf solch eine Warnmeldung reagieren, können Sie festlegen, ob die Aktion immer zugelassen oder verhindert werden soll. Sie sollten die Aktion immer verhindern.

Sygate Personal Firewall (kostenlose und Pro-Version)

Jedes Mal, wenn die Sygate Personal Firewall auf eine neue Aktivität stößt, für die es noch keine Regel gibt, wird eine Eingabeaufforderung angezeigt. Gewähren Sie Zugriff auf die Anwendungen und Speicherorte, auf die Sie mit dem Secure Access Client zugreifen möchten. Klicken Sie auf **Ja**, wenn eine Aufforderung angezeigt wird.

Tiny Personal Firewall

Mit den Tiny Personal Firewall-Einstellungen kann der Secure Access Client eine Verbindung zum Internet und den vom Access Gateway zugelassenen Ressourcen herstellen. Um die Einstellungen zu konfigurieren, öffnen Sie das Verwaltungsfenster der Tiny Personal Firewall und ändern Sie die Einstellungen für die Filterregeln.

Hinweis: Eine Methode zum Konfigurieren der Tiny Personal Firewall besteht darin, auf die Eingabeaufforderungen zu reagieren, die angezeigt werden, wenn die Firewall auf eine neue Aktivität stößt, für die es noch keine Regel gibt. Konfigurieren Sie die Tiny Personal Firewall vor der Installation des Secure Access Clients.

Nachdem Sie die oben genannten Konfigurationsänderungen angewendet und den Secure Access Client gestartet haben, zeigt die Tiny Personal Firewall eine Reihe von Warnmeldungen zu eingehenden Verbindungen an, die sich auf den Secure Access Client beziehen. Sie sollten für jede Warnung die Verbindung zulassen.

ZoneAlarm Pro

Damit der Secure Access Client eine Verbindung zum Internet und den vom Access Gateway zugelassenen Ressourcen herstellen kann, müssen Sie den vollqualifizierten Domänennamen des Geräts als vertrauenswürdige Zone hinzufügen.

Installieren zusätzlicher Access Gateway-Geräte

Sie können in Ihrem Netzwerk mehrere Access Gateway-Geräte installieren. Die zusätzlichen Geräte können sich dabei in einem Cluster oder hinter einem Load Balancer befinden oder sie können für das Failover auf ein anderes Access Gateway im Netzwerk konfiguriert sein.

Wenn Access Gateway-Geräte in einem Cluster angeordnet sind, haben Sie alle dieselben Einstellungen für den Benutzerzugriff auf die internen Netzwerkressourcen. Ein Benutzer kann eine Verbindung zu einem beliebigen Access Gateway im Cluster herstellen und erhält dabei immer die gleichen Zugriffsrechte auf die Ressourcen im internen Netzwerk.

Mit der Installation mehrerer Access Gateway-Geräte können Sie Folgendes erreichen:

- **Skalierbarkeit:** Überschreitet die Anzahl der Benutzer die Kapazität eines einzelnen Access Gateways, können Sie zusätzliche Geräte installieren und so die Arbeitsbelastung bewältigen.
- **Hohe Verfügbarkeit (Failover):** Sie können mehrere Geräte installieren, sodass in jedem Fall ein Access Gateway für die Benutzerverbindungen verfügbar ist, wenn ein anderes Access Gateway ausfällt. Diese Konfiguration gewährt eine hohe Verfügbarkeit des internen Netzwerks für die Remotebenutzer.

Um sowohl Skalierbarkeit als auch Failover zu unterstützen, stellen Sie vor den Access Gateway-Geräten einen Load Balancer bereit. Ein Load Balancer eignet sich in der Regel für größere Unternehmen mit zahlreichen Remotebenutzern. Weitere Informationen hierzu finden Sie unter „Konfigurieren mehrerer Geräte für die Verwendung eines Load Balancers“ auf Seite 275.

Soll nur Failover unterstützt werden, können Sie zwei (oder mehrere) Access Gateway-Geräte bereitstellen und dann ein Gerät mit dem Administration Tool so konfigurieren, dass dieses Gerät das Failover auf bis zu drei weitere Geräte ausführt. Wenn ein Access Gateway ausfällt, werden die Benutzer automatisch mit einem anderen Access Gateway verbunden. Bei dieser Form der Bereitstellung ist kein Load Balancer erforderlich. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Access Gateway-Failover“ auf Seite 280.

Beim Konfigurieren von Lastausgleich und Failover können Sie wahlweise weitere Geräte in den Cluster aufnehmen; dies ist jedoch nicht zwingend erforderlich.

In diesem Kapitel wird vorausgesetzt, dass Sie die folgenden Aufgaben bereits erledigt haben:

- Sie haben auf jedem Access Gateway die TCP/IP-Einstellungen auf der Registerkarte **General Networking** konfiguriert.
- Sie haben auf einem Access Gateway im Netzwerk eine Lizenz installiert (dem *Lizenzserver*).

  Ein Access Gateway im Netzwerk kann als Lizenzserver fungieren. Die Lizenz ist auf einem der Geräte installiert. Die anderen Geräte sind so konfiguriert, dass sie ihre Lizenzen vom Lizenzserver abrufen.
- Sie haben die anderen Geräte so konfiguriert, dass sie eine Verbindung zum Lizenzserver herstellen und die notwendigen Lizenzen abrufen.

  Die anderen im Netzwerk installierten Geräte können auch dann Lizenzen abrufen, wenn sie nicht zum Cluster gehören. Weitere Informationen zur Lizenzierung finden Sie unter „Installieren von Lizenzen“ auf Seite 49.
- Sie haben auf jedem Access Gateway ein signiertes, sicheres Zertifikat von einer Zertifizierungsstelle installiert.

  Jedes Gerät im Cluster muss einen eindeutigen vollqualifizierten Domänennamen besitzen. Werden die Geräte in einem Cluster hinter einem Load Balancer bereitgestellt, muss auf jedem Gerät dasselbe SSL-Serverzertifikat mit demselben vollqualifizierten Domänennamen installiert sein. Falls die Geräte in einem Cluster für Failover konfiguriert sind (ohne sich hinter einem Load Balancer zu befinden), muss auf jedem Gerät ein eindeutiges SSL-Serverzertifikat installiert sein.
- Befinden sich die Geräte in einem Cluster, konfigurieren Sie auf mindestens einem Gerät im Netzwerk die Einstellungen auf den Registerkarten **Access Policy Manager**, **Authentication**, **Global Cluster Policies**, **Portal Page Configuration** und **Group Priority**.

Erstellen eines Clusters mit Access Gateway-Geräten

Wenn Sie mehrere Geräte im Netzwerk nutzen und jedes Gerät dieselben Einstellungen verwendet, können Sie einen Cluster erstellen. Die Einstellungen, die veröffentlicht werden können, werden auf einem Access Gateway konfiguriert und dann für die anderen Geräte veröffentlicht. Alle Geräte im Cluster werden im Administration Tool auf der Registerkarte **Access Gateway Cluster** aufgeführt. Hierdurch lassen sich Konfiguration und Wartung der Geräte im Netzwerk schnell und einfach erledigen.

Die Einstellungen auf der Registerkarte **Access Gateway Cluster** gelten für einzelne Access Gateway-Geräte und werden nicht im Cluster veröffentlicht. Hierzu gehören folgende Einstellungen:

- Allgemeine Netzwerkeinstellungen (Registerkarte **General Networking**)
- Protokollierung (Registerkarte **Logging**)
- Verwaltung (Registerkarte **Administration**)
- Zertifikate (Registerkarte **Certificates**)
- Lizenzierung (Registerkarte **Licensing**)
- Routen (Registerkarte **Routes**)
- Namensdienstanbieter (Registerkarte **Name Service Providers**)
- Failover (Registerkarte **Failover**)
- Datum und Uhrzeit (Registerkarte **Date**)

Die Einstellungen auf den folgenden Registerkarten im Administration Tool werden auf jedem Gerät im Cluster veröffentlicht.

- Access Policy Manager
- Authentication
- Global Cluster Policies
- Portal Page Configuration
- Group Priority

Durch die Veröffentlichung dieser Einstellungen auf den anderen Geräten ist sichergestellt, dass alle Geräte im Cluster dieselben Einstellungen für die Zugriffskontrolle auf die internen Netzwerkressourcen aufweisen.

Bevor Sie ein Gerät in den Cluster aufnehmen, installieren Sie es zunächst gemäß den Anweisungen in Kapitel 4, „Erstmalige Installation des Access Gateways“ auf Seite 39.

Wichtig: Jedes Gerät im Cluster muss dasselbe Administratorkennwort besitzen. Access Gateways mit einem abweichenden Administratorkennwort können nicht im Cluster verwaltet werden. Citrix empfiehlt, das Administratorkennwort während der Installation des Access Gateways mit der seriellen Konsole zu ändern. Weitere Informationen finden Sie unter „Konfigurieren der TCP/IP-Einstellungen mit dem seriellen Kabel“ auf Seite 42 und „Konfigurieren des Administratorkennworts“ auf Seite 258.

Das neue Kennwort muss zwischen 6 und 127 Zeichen enthalten. Kennwörter dürfen nicht mit einem Leerzeichen beginnen oder enden.

So fügen Sie dem Cluster Geräte hinzu:

1. Öffnen Sie das Administration Tool auf dem primären Access Gateway.
2. Klicken Sie auf die Registerkarte **Access Gateway Cluster**.
3. Geben Sie unter **Add an Access Gateway to the Cluster** in das Feld **FQDN** den vollqualifizierten Domänennamen für ein zusätzliches Access Gateway ein und klicken Sie auf **Add**.
4. Wiederholen Sie Schritt 1 bis 3 für alle Geräte im Cluster.

Sobald Sie alle Geräte in den Cluster aufgenommen haben, können Sie die Einstellungen vom primären Access Gateway im Cluster veröffentlichen.

So veröffentlichen Sie die Einstellungen von einem Gerät auf den anderen Geräten im Cluster:

1. Klicken Sie im Administration Tool auf dem ersten installierten Access Gateway (dem primären Gerät) auf die Registerkarte **Publish**.
2. Klicken Sie auf **Publish**. Die Einstellungen des ersten Access Gateways werden auf allen Access Gateway-Geräten im Cluster veröffentlicht.
3. Klicken Sie auf die Registerkarte **Access Gateway Cluster** und anschließend auf die Registerkarte **Administration**.
4. Klicken Sie im Bereich **Access Gateway management** neben **Restart the appliance** auf **Restart**.

Nach der Veröffentlichung der Konfigurationseinstellungen auf allen Geräten im Cluster müssen alle Access Gateway-Geräte neu gestartet werden, damit die Änderungen in Kraft treten.

Jedes Access Gateway im Cluster wird auf der Registerkarte **Publish** aufgeführt. Im Feld **Synchronization Status** wird für jedes Gerät eine der folgenden Synchronisierungsmeldungen angezeigt:

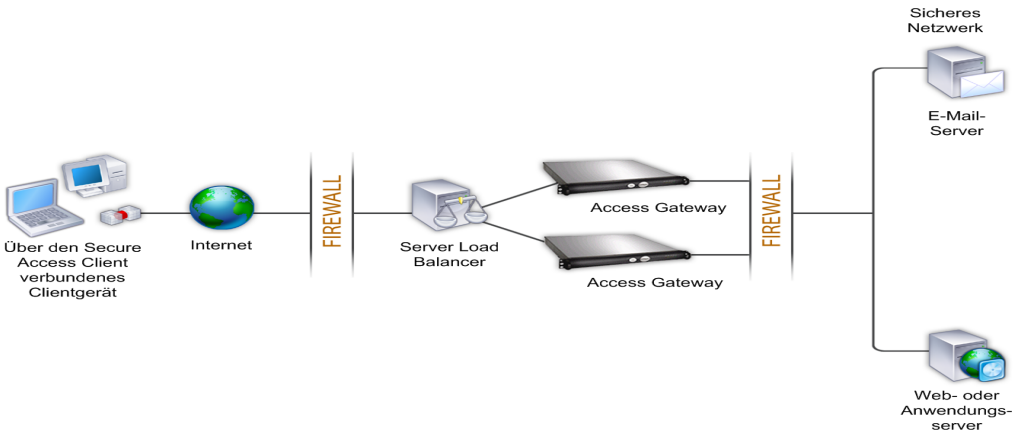
- **In Sync:** Die Access Gateway-Konfiguration wurde erfolgreich veröffentlicht.
- **Not in Sync:** Die Einstellungen wurden geändert, aber nicht veröffentlicht.
- **Sync Failed:** Die Synchronisierung des Access Gateways ist fehlgeschlagen. Überprüfen Sie das Gerät und versuchen Sie es dann erneut.
- **Unknown Status:** Der Status des Access Gateways kann nicht ermittelt werden. Überprüfen Sie das Gerät und versuchen Sie es dann erneut.

Konfigurieren mehrerer Geräte für die Verwendung eines Load Balancers

Durch die Bereitstellung mehrerer Geräte hinter einem Load Balancer können Sie eine große Anzahl Remotebenutzer unterstützen und dabei die hohe Verfügbarkeit des internen Netzwerks für die Benutzer sicherstellen.

Der gemeinsam mit den Geräten bereitgestellte Load Balancer muss den Lastausgleich auf der Grundlage der Ursprungs-IP-Adresse (Src IP) oder der SSL-Sitzungs-IDs (SSL ID) unterstützen.

.



Mehrere Access Gateway-Geräte hinter einem Load Balancer

Der Load Balancer ist mit einer eindeutigen IP-Adresse oder einem eindeutigen vollqualifizierten Domänennamen konfiguriert. Der Secure Access Client, ein

Webbrowser oder Kioskverbindungen greifen über diese Adresse auf den Load Balancer zu. Der Load Balancer verteilt die Clientverbindungen gleichmäßig auf die Geräte, die hinter ihm bereitgestellt sind.

Sobald eine Clientverbindung eingeht, wählt der Load Balancer mithilfe eines Algorithmus eines der Geräte in der Liste aus und leitet die Clientverbindung an das ausgewählte Access Gateway weiter.

Neben der gleichmäßigen Verteilung der Clientverbindungen trägt ein Load Balancer auch zur hohen Verfügbarkeit des internen Netzwerks bei.

Einige Load Balancer sind in der Lage, den Ausfall von Geräten zu erkennen, die sich hinter ihnen befinden. Wenn ein Load Balancer erkennt, dass ein Gerät ausgefallen ist, entfernt der Load Balancer das betreffende Gerät aus der Liste der verfügbaren Geräte und leitet die Clientverbindungen an die verbleibenden aktiven Geräte um. Sobald das Access Gateway wieder online ist, wird es durch den Load Balancer wieder in die Liste der aktiven Geräte aufgenommen. So wird sichergestellt, dass alle Clientverbindungen auch dann ununterbrochen Zugriff auf das interne Netzwerk erhalten, wenn ein Access Gateway ausfällt.

Konfigurieren des Lastausgleichs

Installieren und konfigurieren Sie den Load Balancer gemäß der Dokumentation des Herstellers in der DMZ des Netzwerks.

Die folgenden Konfigurationsschritte sind erforderlich, damit der Load Balancer mit den Access Gateway-Geräten zusammenarbeitet:

- Konfigurieren Sie den Load Balancer für den Lastausgleich von Verbindungen zu den Access Gateway-Geräten auf der Grundlage der Ursprungs-IP-Adressen (Src IP) oder der SSL-Sitzungs-IDs (SSL ID). Um die bestmögliche Leistung zu erzielen, sollten Sie den Lastausgleich mit SSL ID konfigurieren.
- Konfigurieren Sie den Load Balancer mit einem vollqualifizierten Domänennamen, den das Access Gateway beim Aufbauen der Verbindung zum Load Balancer verwenden soll.
- Konfigurieren Sie den Load Balancer so, dass die SSL-Verschlüsselung nicht beendet wird. Die SSL-Verbindung muss an das Access Gateway übergeben werden; dort erst darf die SSL-Verschlüsselung beendet werden.

Konfigurieren von Access Gateway-Geräten für den Betrieb hinter einem Load Balancer

Im Anschluss an die Installation und Konfiguration des Load Balancers gehen Sie bei den Access Gateway-Geräten, die sich hinter dem Load Balancer befinden, wie folgt vor:

- Schließen Sie für jedes Access Gateway die Netzwerkkabel so an, dass das Interface 0 mit dem Load Balancer verbunden ist und das Interface 1 mit dem internen Netzwerk.
- Konfigurieren Sie die Access Gateway-Geräte hinter dem Load Balancer für den Betrieb als Cluster. Mit einem Cluster stellen Sie sicher, dass alle Access Gateway-Geräte so konfiguriert sind, dass sie den Zugriff auf die Netzwerkressourcen auf dieselbe Weise unterstützen. Über den Load Balancer kann der Benutzer mit jedem Access Gateway im Cluster eine Verbindung herstellen und erhält dabei jeweils dieselben Zugriffsrechte. Weitere Informationen hierzu finden Sie unter „Erstellen eines Clusters mit Access Gateway-Geräten“ auf Seite 273.
- Erstellen Sie ein einzelnes SSL-Serverzertifikat im PEM-Format und den zugehörigen privaten Schlüssel und laden Sie dieses Zertifikat und den Schlüssel auf alle Access Gateway-Geräte hoch. Weitere Informationen hierzu finden Sie unter „Erstellen eines Zertifikats für Geräte hinter einem Load Balancer“ auf Seite 277.

Erstellen eines Zertifikats für Geräte hinter einem Load Balancer

Wenn Sie Access Gateway-Geräte hinter einem Load Balancer bereitstellen, müssen dasselbe SSL-Serverzertifikat und derselbe private Schlüssel auf jedem einzelnen Gerät zur Verfügung gestellt werden.

Wichtig: Erstellen Sie die SSL-Serverzertifikatsanforderung nicht mit der Funktion **Certificate Signing Request** auf der Registerkarte **Access Gateway Cluster** im Administration Tool. Diese Funktion erzeugt einen eigenen privaten Schlüssel auf dem Access Gateway, auf dem sie ausgeführt wird. Wenn Access Gateway-Geräte hinter einem Load Balancer bereitgestellt sind, muss jedes Access Gateway denselben privaten Schlüssel und dasselbe SSL-Zertifikat verwenden.

So erstellen Sie ein SSL-Serverzertifikat und einen privaten Schlüssel:

1. Erstellen Sie die SSL-Serverzertifikatsanforderung und den privaten Schlüssel mit einem OpenSSL-Tool, beispielsweise mit Keytool. (Weitere Informationen zu OpenSSL und den verfügbaren Tools finden Sie im Internet unter http://www.openssl.org/.)

   - Erstellen Sie das Serverzertifikat im PEM-Format.
   - Geben Sie den vollqualifizierten Domänennamen des Load Balancers als Servernamen in der Serverzertifikatsanforderung an, nicht den vollqualifizierten Domänennamen eines der Access Gateway-Geräte.

     Optional können Sie ein Sternchen (*) anstelle des Servernamens im vollqualifizierten Domänennamen in der Serverzertifikatsanforderung angeben. Beispiel:

     ***.domäne.com**
   - Erstellen Sie den privaten Schlüssel getrennt von der Serverzertifikatsanforderung.

2. Senden Sie die SSL-Serverzertifikatsanforderung zur Signierung an eine Zertifizierungsstelle. Senden Sie dabei ausschließlich das Serverzertifikat im PEM-Format, nicht jedoch den privaten Schlüssel.
3. Sobald Sie die signierte SSL-Serverzertifikatsanforderung von der Zertifizierungsstelle erhalten, tragen Sie den privaten Schlüssel manuell oben im signierten Zertifikat ein. Weitere Informationen zum Eintragen eines privaten Schlüssels in ein signiertes Zertifikat finden Sie unter „Kombinieren des privaten Schlüssels mit dem signierten Zertifikat“ auf Seite 304.
4. Laden Sie das SSL-Serverzertifikat und den privaten Schlüssel auf alle Access Gateway-Geräte hinter dem Load Balancer hoch.

   A. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.

   B. Klicken Sie auf die Registerkarte **Administration**.

   C. Klicken Sie neben **Upload a .pem private key and signed certificate** auf die Schaltfläche **Browse**.

   D. Navigieren Sie zu der Datei, in der sich das signierte, mit dem privaten Schlüssel versehene PEM-Zertifikat befindet, markieren Sie diese Datei und klicken Sie auf **Öffnen**.

   Wiederholen Sie Schritt 4 für alle Access Gateway-Geräte hinter dem Load Balancer und laden Sie jeweils den privaten Schlüssel und das PEM-Zertifikat auf die einzelnen Access Gateway-Geräte hoch.

Festlegen eines Load Balancers als Standardgateway

Bei einigen Load Balancern oder Netzwerkkonfigurationen muss der Load Balancer als Standardgateway für das Access Gateway festgelegt werden. Wenn Sie den Load Balancer als Standardgateway festlegen, konfigurieren Sie statische Routen auf dem Access Gateway, sodass der gesamte Datenverkehr, der für das sichere Netzwerk bestimmt ist, an ein internes Netzwerk weitergeleitet wird, das diesen internen Datenverkehr problemlos bewältigen kann.

Erhält das Access Gateway ein Paket, das an eine unbekannte IP-Adresse gerichtet ist, wird dieses Paket an die Adresse des Standardgateways übermittelt. Wenn der Load Balancer als Standardgateway konfiguriert ist, sorgt das Access Gateway mit statischem Routing dafür, dass die für die internen Ziele bestimmten Pakete tatsächlich ausgeliefert werden.

Falls das Access Gateway ein Paket empfängt, das für eine interne Adresse bestimmt ist, ohne dass die statische Routingtabelle eine geeignete Route für das Paket aufweist, geht das Paket unter Umständen verloren.

Beispiel: Der Load Balancer ist als Standardgateway konfiguriert und es gilt Folgendes:

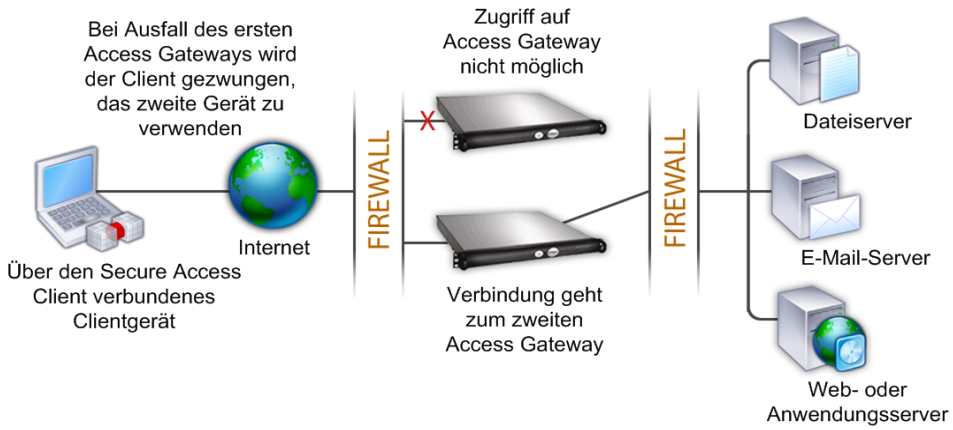
- Sie verwenden drei interne Netzwerke: 10.10.0.0, 10.20.0.0 und 10.30.0.0.
- Das Netzwerk 10.10.0.0 kann Pakete an die Netzwerke 10.20.0.0 und 10.30.0.0 weiterleiten; diese Netzwerke können jedoch ihrerseits keine Pakete an andere Netzwerke übermitteln.

In dieser Umgebung müssen auf dem Access Gateway statische Routen für Interface 1 erstellt werden. Diese statischen Routen müssen den gesamten Datenverkehr, der für die Netzwerke 10.20.0.0 und 10.30.0.0 bestimmt ist, über Interface 1 am Access Gateway an das Netzwerk 10.10.0.0 weiterleiten.

Weitere Informationen hierzu finden Sie unter „Konfigurieren von dynamischen und statischen Routen“ auf Seite 64.

Konfigurieren von Access Gateway-Failover

Um hohe Verfügbarkeit des internen Netzwerks für Remotebenutzer zu gewährleisten, können Sie zwei oder mehrere Access Gateway-Geräte bereitstellen und für gegenseitiges Failover konfigurieren. In dieser Bereitstellung steht stets ein alternatives Access Gateway zur Verfügung, wenn ein Access Gateway ausfällt. Da das Access Gateway-Failover aktiv/aktiv ist, kann jedes Access Gateway als primäres Gateway für eine andere Gruppe von Benutzern verwendet werden.


Bei Ausfall des ersten Access Gateways wird der Client gezwungen, das zweite Gerät zu verwenden
Zugriff auf Access Gateway nicht möglich
FIREWALL
FIREWALL
Dateiserver
E-Mail-Server
Internet
Über den Secure Access Client verbundenes Clientgerät
Verbindung geht zum zweiten Access Gateway
Web- oder Anwendungsserver

Mehrere Access Gateway-Geräte sorgen für Failover

Wenn ein Access Gateway für Failover konfiguriert ist, liefert das Access Gateway eine Failoverliste an den Secure Access Client.

Wenn der Secure Access Client das erste Mal eine Verbindung herstellt, erhält er vom Access Gateway die Failoverliste. Sobald der Client die Verbindung zum primären Access Gateway verliert, geht er die Liste der Failovergeräte durch. Wenn das primäre Access Gateway ausfällt, versucht der Client 20 Sekunden lang, die Verbindung wiederherzustellen. Wenn diese Versuche fehlschlagen, wird die Verbindung anhand der Angaben in der Failoverliste hergestellt. Der Client führt eine DNS-Suche nach dem ersten Failovergerät durch und versucht, eine Verbindung mit diesem Gerät herzustellen. Wenn das erste Failover-Access Gateway-Gerät nicht verfügbar ist, versucht es der Client mit dem nächsten Failovergerät. Gelingt es dem Client, eine Verbindung zu einem Failover-Access Gateway herzustellen, wird er aufgefordert, sich anzumelden.

Sie können bis zu drei Access Gateway-Geräte in die Failoverliste eintragen.

So konfigurieren Sie Failover:

1. Klicken Sie auf die Registerkarte **Access Gateway Cluster** und anschließend auf die Registerkarte **Failover Servers**.
2. Geben Sie in den Feldern **First failover appliance**, **Second failover appliance** und/oder **Third failover appliance** die externen IP-Adressen oder die vollqualifizierten Domänennamen der Access Gateways ein, die für Failover verwendet werden sollen.

   Die Access Gateway-Geräte werden in der Reihenfolge für das Failover herangezogen, in der sie in der Liste aufgeführt sind.
3. Geben Sie im Feld **Port** die Portnummer ein. Der Standardwert ist 443. Klicken Sie auf **Submit**.

Hinweis: Wenn Sie mehrere Access Gateway-Geräte hinter einem Load Balancer bereitstellen, müssen dasselbe SSL-Serverzertifikat und derselbe private Schlüssel auf jedem einzelnen Access Gateway installiert werden. Sollen mehrere Access Gateway-Geräte für Failover eingesetzt werden, können Sie auf diesen Geräten nicht dasselbe SSL-Serverzertifikat verwenden. In diesem Fall müssen Sie jeweils ein anderes SSL-Serverzertifikat auf den einzelnen Access Gateway-Geräten installieren. Sie können die SSL-Zertifikatsanforderung für die Access Gateway-Failovergeräte mit der Funktion **Certificate Signing Request** im Administration Tool erstellen. Weitere Informationen hierzu finden Sie unter „Erstellen und Installieren von Zertifikaten“ auf Seite 55.

Überwachen des Access Gateways

In den folgenden Themen wird beschrieben, wie Sie die Access Gateway-Protokolle und Netzwerküberwachungstools für das Access Gateway verwenden:

- Anzeigen und Herunterladen von Systemmeldungsprotokollen
- Aktivieren und Anzeigen von SNMP-Protokollen
- Anzeigen von Systemstatistiken
- Überwachen der Access Gateway-Operationen

Anzeigen und Herunterladen von Systemmeldungsprotokollen

Für das Access Gateway gibt es zwei Arten der Protokollierung. Sämtliche Protokolle werden lokal gespeichert und können im Administration Tool oder im Administration Portal angezeigt werden. Bei Bedarf können diese Informationen auch an einen Systemprotokollserver gesendet werden.

Systemmeldungsprotokolle enthalten Informationen, die den Access Gateway-Supportmitarbeitern die Fehlersuche und -beseitigung erleichtern können. Durch Prüfung der bereitgestellten Informationen können Sie Änderungen verfolgen, die sich u. U. negativ auf die Stabilität und Leistung des Access Gateways auswirken.

Systemmeldungsprotokolle werden auf dem Access Gateway für die Dauer von 30 Tagen archiviert. Das älteste Protokoll wird dann jeweils durch das aktuelle Protokoll ersetzt.

Sie können jederzeit einzelne oder auch alle Protokolle herunterladen. Sie können Systemmeldungen auch an Ihren Systemprotokollserver weiterleiten. Informationen hierzu finden Sie unter „Weiterleiten von Systemmeldungen an einen Systemprotokollserver“ auf Seite 286.

Hinweis: Wenn Sie über das Administration Tool keine Verbindung zum Access Gateway herstellen können, gehen Sie zum Administration Portal und klicken Sie auf die Registerkarte **Logging**.

So können Sie das Systemprotokoll anzeigen und filtern:

1. Öffnen Sie auf der Registerkarte **Access Gateway Cluster** das Fenster für das Access Gateway.
2. Klicken Sie auf **Logging/Settings**.
3. Klicken Sie unter **Gateway log** auf **Show Log File**.

   Das Protokoll für das aktuelle Datum wird angezeigt.

   Wenn Sie das Protokoll für ein früheres Datum anzeigen möchten, wählen Sie in der Liste **Log archive** das entsprechende Datum aus und klicken Sie dann auf **View Log**.
4. Standardmäßig werden im Protokoll alle Einträge angezeigt. Das Protokoll kann aber wie folgt gefiltert werden:

   - Wählen Sie im Bereich **Log Filters** unter **Log Type** entweder **Administrators**, **System Applications** oder **Users** aus.
   - Um nach Priorität zu filtern, wählen Sie im Bereich **Log Filters** entweder **Low**, **Medium**, **High** oder **Critical** aus.

     Die ausgewählten Filter werden als logisches ODER behandelt. Das bedeutet, dass für jeden ausgewählten Filter sämtliche übereinstimmenden Einträge angezeigt werden.
5. So laden Sie ein Protokoll herunter:

   - Wählen Sie in der Liste **Log Archive** ein Protokoll aus und klicken Sie neben **Selected Log File** auf **Download**. Der Protokolldateiname hat standardmäßig folgendes Format: *JJJJMMTT*.log.
   - Wenn Sie alle Protokolle herunterladen möchten, klicken Sie neben **All Log Files** auf **Download**. Der Dateiname lautet dann standardmäßig wie folgt: log_archive_*JJJJMMTT*.tgz. Zum Herunterladen von Protokollen vom Access Gateway muss auf Ihrem Computer ein Datenkomprimierungsprogramm, z. B. WinZip, installiert sein. Die Protokolle werden als .tgz-Datei heruntergeladen und müssen dann

extrahiert werden. Nach dem Herunterladen einer Datei können Sie deren Inhalt extrahieren und so auf die einzelnen Protokolldateien zugreifen.

Anzeigen von Secure Access Client-Verbindungsprotokollen

Das Secure Access-Verbindungsprotokoll enthält Echtzeitinformationen zu Verbindungen. Diese Informationen sind besonders für die Fehlersuche bei Verbindungsproblemen des Secure Access Clients wichtig. Sie können über das Secure Access Client-Symbol vom Clientgerät auf das Verbindungsprotokoll zugreifen. Der Benutzer kann Ihnen diese Informationen für die Fehlersuche bei Verbindungsproblemen schicken.

So zeigen Sie das Verbindungsprotokoll an:

1. Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Secure Access Client-Symbol.
2. Wählen Sie im Kontextmenü den Befehl **Verbindungsprotokoll**.

   Das Verbindungsprotokoll für die Sitzung wird geöffnet.

Hinweis: Der Pfad zum Verbindungsprotokoll auf dem Computer des Benutzers lautet: *systemroot*\Dokumente und Einstellungen*Benutzername*\Lokale Einstellungen\Anwendungsdaten\NET6\net6vpn.log. Das Protokoll wird bei jedem Einrichten einer neuen VPN-Verbindung überschrieben.

Citrix empfiehlt, die Benutzer aufzufordern, das Verbindungsprotokoll im ausführlichen Modus zu erstellen, da auf diese Weise detaillierte Informationen für die Problembehandlung, z. B. die Zertifikatsüberprüfung, zur Verfügung stehen.

So legen Sie ausführlichen Modus für das Clientverbindungsprotokoll fest:

1. Klicken Sie mit der rechten Maustaste auf das Secure Access Client-Symbol und klicken Sie dann auf **Verbindungsprotokoll**.
2. Aktivieren Sie im Menü **Optionen** die Option **Ausführlicher Modus**.

Weiterleiten von Systemmeldungen an einen Systemprotokollserver

Das Access Gateway archiviert Systemmeldungen. Informationen hierzu finden Sie unter „Anzeigen und Herunterladen von Systemmeldungsprotokollen“ auf Seite 283. Sie können das Access Gateway aber auch anweisen, Systemmeldungen an einen Systemprotokollserver weiterzuleiten.

So leiten Sie Access Gateway-Systemmeldungen an einen Systemprotokollserver weiter:

1. Klicken Sie auf die Registerkarte **Access Gateway Cluster** und anschließend auf die Registerkarte **Logging/Settings**.
2. Geben Sie unter **Syslog Settings** im Feld **Server** die IP-Adresse des Systemprotokollservers ein.
3. Wählen Sie im Feld **Facility** die gewünschte Systemprotokollstufe aus.
4. Geben Sie im Feld **Broadcast interval (mins)** eine Sendefrequenz in Minuten ein. Wenn Sie hier **0** eingeben, erfolgt die Protokollierung fortlaufend. Klicken Sie auf **Submit**.

Aktivieren und Anzeigen von SNMP-Protokollen

Wenn SNMP (Simple Network Management Protocol) aktiviert ist, meldet das Access Gateway die MIB-II-Systemgruppe (1.3.6.1.2.1). Das Access Gateway unterstützt keine Access Gateway-spezifischen SNMP-Daten.

Sie können ein SNMP-Überwachungstool, z. B. Multi Router Traffic Grapher, konfigurieren, um vom Access Gateway gemeldete SNMP-Daten grafisch darzustellen. Ein Beispiel für eine MRTG-Ausgabe finden Sie unter „Beispiel für eine MRTG-Ausgabe“ auf Seite 287.

So aktivieren Sie die Protokollierung von SNMP-Meldungen:

1. Klicken Sie auf die Registerkarte **Access Gateway Cluster** und anschließend auf die Registerkarte **Logging/Settings**.
2. Wählen Sie unter **SNMP settings** die Option **Enable SNMP**.
3. Geben Sie unter **Location** den SNMP-Speicherort ein. Dieses Feld dient nur zur Information.

4. Geben Sie unter **Contact** den Kontakt ein. Dieses Feld dient nur zur Information.
5. Geben Sie unter **Community** die Community ein. Dieses Feld dient nur zur Information.
6. Geben Sie unter **Port** die Portnummer an. Klicken Sie auf **Submit**.

Beispiel für eine MRTG-Ausgabe

Multi Router Traffic Grapher (MRTG) ist ein Tool zur Überwachung von SNMP-Daten (Verkehrslast usw.). MRTG generiert HTML-Seiten mit PNG-Bildern zur visuellen Darstellung des Verkehrs. Das Tool funktioniert unter UNIX, Windows 2000 Server und Windows Server 2003.

Hinweis: Die Informationen in diesem Abschnitt geben einen allgemeinen Überblick über das Arbeiten mit MRTG. Weitere Informationen zur Beschaffung und Verwendung dieses Tools finden Sie auf der Website von Multi Router Traffic Grapher unter http://people.ee.ethz.ch/~oetiker/webtools/mrtg/.

So erfassen Sie SNMP-Daten für das Access Gateway über MRTG (in UNIX):

1. Konfigurieren Sie das Access Gateway für das Antworten auf SNMP-Abfragen. Informationen hierzu finden Sie unter „So aktivieren Sie die Protokollierung von SNMP-Meldungen:“ auf Seite 286.
2. Erstellen Sie die MRTG-Konfigurationsdateien in /etc/mrtg.

   Die Konfigurationsdateien enthalten Angaben dazu, welche Objekt-IDs vom MRTG-Daemon überwacht werden sollen, von welchem Ziel die SNMP-Daten bezogen werden sollen und wie die MRTG-Ausgabe aussehen soll.

```
WorkDir: /var/www/html/mrtg
Options[_]: nopercent,gauge,noinfo,growright

Target[vpn.myorg.com.tcpCurrEstab]: .1.3.6.1.2.1.6.9.0&.1.3.6.1.2.1.6.9.0:mypswd@10.10.0.30
Xsize[vpn.myorg.com.tcpCurrEstab]: 600
Ysize[vpn.myorg.com.tcpCurrEstab]: 200
Ytics[vpn.myorg.com.tcpCurrEstab]: 10
Title[vpn.myorg.com.tcpCurrEstab]: ESTABLISHED TCP connections
PageTop[vpn.myorg.com.tcpCurrEstab]: <h1>ESTABLISHED TCP connections</h1>
MaxBytes[vpn.myorg.com.tcpCurrEstab]: 1000000
YLegend[vpn.myorg.com.tcpCurrEstab]: # est. conns
ShortLegend[vpn.myorg.com.tcpCurrEstab]:  
LegendI[vpn.myorg.com.tcpCurrEstab]:  Connections: 
LegendO[vpn.myorg.com.tcpCurrEstab]:
Legend1[vpn.myorg.com.tcpCurrEstab]: Established TCP connections
```

MRTG-Konfigurationsdatei

3. Bearbeiten Sie /etc/crontab so, dass alle 5 Minuten eine SNMP-Abfrage durchgeführt wird, anhand derer eine grafische Ausgabe erstellt werden kann. Die einzelnen aufgeführten CFG-Dateien generieren eine separate Ausgabe.
4. Zeigen Sie die Ausgabe in einem Webbrowser an.

   Das Tool speichert die HTML-Ausgabe in dem in der Konfigurationsdatei angegebenen Arbeitsverzeichnis. Der Dateiname der Ausgabe, der mit dem der in Schritt 2 erstellten Konfigurationsdatei übereinstimmt, lautet vpn.myorg.com.tcpcurrestab.html.

Anzeigen von Systemstatistiken

Klicken Sie zum Abrufen allgemeiner statistischer Systeminformationen auf die Registerkarte **Access Gateway Cluster** und dann auf die Registerkarte **Statistics**.

Die statistischen Angaben bieten einen Überblick über das Access Gateway und enthalten folgende Informationen:

- Die Version des Access Gateways.
- Dauer der Ausführung des Access Gateways.
- Speichernutzung.
- Maximale und verwendete Verbindungen: Die Angabe der maximalen Verbindungen steht für die Anzahl der Lizenzen, die für die Verwendung mit dem Access Gateway verfügbar sind.
- Anmeldeinformationen für Administratoren, Secure Access Client-Verbindungen und Kioskverbindungen.

Überwachen der Access Gateway-Operationen

Das Access Gateway enthält eine Reihe von Linux-Standardüberwachungs-anwendungen, sodass Sie bequem von einem zentralen Standort aus auf die Anwendungen zugreifen können. Mit Ausnahme des von Citrix entwickelten Real-time Monitors unterliegen die im Access Gateway enthaltenen Anwendungen der öffentlichen GNU-Lizenz.

Die Überwachungsanwendungen befinden sich auf dem Administration Desktop. Über die Symbole auf dem Bildschirm unten links können Sie mit einem einzigen Mausklick auf die sechs vorhandenen Überwachungstools zugreifen. Der rechten unteren Ecke können Sie die Prozess- und Netzwerkaktivitätsstufen entnehmen. Gehen Sie zum Anzeigen numerischer Daten mit der Maus über die beiden Diagramme.

So öffnen Sie den Administration Desktop:

1. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse oder den FQDN des Access Gateways ein. Folgende Formate werden akzeptiert: https://*FQDN*:9001 oder https://*IP-Adresse*:9001.
2. Klicken Sie im Administration Portal auf **Downloads**.
3. Klicken Sie unter **Access Gateway Administration Desktop** auf **Launch the Access Gateway Administration Desktop**.
4. Geben Sie im Dialogfeld **Citrix Access Gateway Remote Admin Desktop** einen Administratorbenutzernamen und das entsprechende Kennwort ein.

Folgende Überwachungsanwendungen stehen zur Verfügung:

- **Citrix Real-time Monitor:** Zeigt die offenen Clientverbindungen an. Wenn Sie sich die Details zu einer Verbindung ansehen möchten, klicken Sie auf den Pfeil für den entsprechenden Benutzernamen.

  Vom Monitor aus können Sie eine Verbindung nach Verbindungstyp (TCP usw.) vorübergehend schließen und einen Benutzer deaktivieren (der Benutzer kann erst wieder eine Verbindung herstellen, wenn Sie ihn wieder aktiviert haben) und wieder aktivieren. Weitere Informationen hierzu finden Sie unter „Schließen und Deaktivieren von Benutzerverbindungen“ auf Seite 173.

- **Ethereal Network Analyzer:** Ermöglicht es Ihnen, interaktiv Paketdaten aus einem aktiven Netzwerk oder aus einer zuvor gespeicherten Erfassungsdatei zu durchsuchen. Weitere Informationen finden Sie in der Hilfe im Ethereal Network Analyzer-Fenster.

- **xNetTools:** Multithread-Netzwerktool, das einen Dienstscanner, einen Portscanner, ein Dienstprogramm zum Pingen, einen Pingscan, einen Namensscan, eine whois-Abfrage und eine Fingerabfrage beinhaltet. Sie finden diese Tools im Menü **Tools**.

- **Traceroute:** Kombiniert die Funktionalität der Befehle **traceroute** und **ping** in einem Netzwerkdiagnosetool. Wenn Traceroute gestartet wird, untersucht das Tool die Netzwerkverbindung zwischen dem Access Gateway und dem von Ihnen festgelegten Zielhost. Nachdem das Tool die Adresse der einzelnen Netzwerkhops zwischen den Geräten bestimmt hat, sendet es eine ICMP ECHO-Sequenzanforderung an alle, um die Qualität der einzelnen Verbindungen zu den Geräten festzustellen. Dabei druckt es fortlaufende Statistiken zu den einzelnen Geräten.

- **fnetload:** Stellt Netzwerkschnittstellenstatistiken in Echtzeit bereit. Das Tool überprüft /proc/net/dev einmal pro Sekunde und stellt die ermittelten Werte grafisch dar.
- **Gnome System Monitor:** Zeigt Informationen zur CPU-Nutzung und zur Nutzung des Arbeitsspeichers und des Auslagerungsbereichs an. Weitere Informationen finden Sie in der Hilfe im System Monitor-Fenster.

Wenn Sie Netzwerküberwachungstools wie Netstat, TCPView oder NetMon auf dem Client verwenden, treten unter Umständen eingehende TCP-Verbindungen vom Access Gateway auf willkürlichen hohen Ports auf. Diese Verbindungen finden nicht wirklich statt. Sie werden von der NDIS shim-Komponente initiiert.

Aus diesem Grund müssen IP-Firewall-Regeln für den Client festgelegt sein, um Datenverkehr vom und zum Access Gateway sowie zu Ziel-IP-Adressen zu ermöglichen. Lokal, also auf dem Clientcomputer, wird der gesamte verbindungsspezifische Verkehr (wie SYN-ACK-, PUSH-, ACK- und FIN-Pakete) vom Secure Access Client neu erstellt, damit es so aussieht, als käme er vom privaten Server. Der Client sendet physischen Datenverkehr nur über Port 443 an das Gateway.

Bei der Clientinitialisierung sind fünf UDP-Socketverbindungen sichtbar. Es handelt sich um folgende Verbindungen:

- 10000 UDP steuert die Informationen zwischen dem Netzwerktreiber und der Portweiterleitung.
- 10010 TCP/UPD ist die Datennutzlast.
- 10020 UDP wird für DNS verwendet.
- 10030 UDP wird für ICMP verwendet.
- 10040 UDP ist für zukünftige Verwendung reserviert.

Sichern von Verbindungen mit digitalen Zertifikaten

Dieses Kapitel enthält eine Übersicht der in der Access Gateway-Lösung verwendeten Sicherheitstechnologien und soll Ihnen helfen, Anzahl und Typ der jeweils erforderlichen Zertifikate zu ermitteln und zu entscheiden, wie und wo Sie diese erhalten und installieren. Dieser Anhang enthält die folgenden Themen:

- Einführung in Sicherheitsprotokolle, Kryptografie und digitale Zertifikate
- Beantragen von Zertifikaten
- Beantragen von Serverzertifikaten
- Verwenden von Windows-Zertifikaten
- Anfordern von Zertifikaten für interne Verbindungen
- Verwenden von Platzhalterzertifikaten

Wichtig: Verwenden Sie zum Konfigurieren von Zertifikaten keine 512-Bit-Schlüsselpaare, da diese oft Opfer von Brute-Force-Angriffen werden.

Einführung in Sicherheitsprotokolle, Kryptografie und digitale Zertifikate

Dieser Abschnitt enthält eine Einführung in das SSL (Secure Sockets Layer)- und das TSL (Transport Layer Security)-Protokoll und bietet einen Überblick über Kryptografie und die Public Key Infrastructure (PKI).

Einführung in Sicherheitsprotokolle

SSL und TLS sind die führenden Internet-Sicherheitsprotokolle für E-Commerce, Webdienste und eine Vielzahl anderer Netzwerkfunktionen.

Das SSL-Protokoll ist der aktuelle Standard für den sicheren Informationsaustausch im Internet. Dieses ursprünglich von Netscape entwickelte Protokoll wurde enorm wichtig für den Internetbetrieb. Daher übernahm die IETF (Internet Engineering Taskforce) die Aufgabe, SSL als offenen Standard zu entwickeln. Um SSL von anderen Entwicklungsarbeiten zu unterscheiden, wurde SSL von der IETF in TLS umbenannt. Das TLS-Protokoll stammt von der dritten SSL-Version ab, wobei TLS 1.0 SSL 3.1 entspricht.

Einige Organisationen, u. a. amerikanische Regierungsstellen, verlangen das Sichern der Datenkommunikation mit TLS. Diese Organisationen verlangen u. U. auch die Verwendung verifizierter Kryptografie. FIPS (Federal Information Processing Standard) 140 ist ein Kryptografiestandard.

Mit dem SSL/TLS-Protokoll können sicherheitskritische Daten über öffentliche Netzwerke, wie das Internet, übertragen werden. Dieses Protokoll bietet die folgenden wichtigen Sicherheitsfunktionen:

Authentifizierung: Ein Client kann die Identität eines Servers ermitteln und feststellen, dass der Server kein Betrüger ist. Optional kann ein Server auch die Identität des Clients authentifizieren, der Verbindungen anfordert.

Datenschutz: Die zwischen dem Client und dem Server übertragenen Daten werden verschlüsselt, damit sie nicht entschlüsselt werden können, falls Nachrichten von Dritten abgefangen werden.

Datenintegrität: Der Empfänger verschlüsselter Daten weiß, ob diese von einem Dritten manipuliert oder geändert wurden.

Einführung in die Kryptografie

Für die sichere Datenübertragung nutzt das SSL/TLS-Protokoll *Kryptografie*. Mit Kryptografie können Nachrichten verschlüsselt werden, um die Vertraulichkeit zu gewährleisten. Kryptografie dient auch zur Authentifizierung der Identität einer Nachrichtenquelle und zur Gewährleistung der Integrität ihres Inhalts.

Nachrichten werden mit einem Geheimcode, einer sogenannten *Verschlüsselungssammlung*, übertragen. Mit der Verschlüsselungssammlung wird eine Nachricht verschlüsselt, damit sie nur vom Absender und Empfänger verstanden werden kann. Da nur der Empfänger, der den Geheimcode hat, die ursprüngliche Nachricht entschlüsseln kann, ist die Vertraulichkeit gewährleistet.

Mit Kryptografie kann der Absender spezielle Informationen in eine Nachricht aufnehmen, die nur dem Absender und Empfänger bekannt sind. Der Empfänger kann die Nachricht durch Prüfen dieser speziellen Informationen authentifizieren.

Durch Kryptografie ist auch gewährleistet, dass der Inhalt einer Nachricht nicht geändert wird. Zu diesem Zweck schließt der Absender einen kryptografischen Vorgang namens *Hashfunktion* in die Nachricht ein. Eine Hashfunktion ist eine mathematische Darstellung der Informationen und lässt sich mit den Prüfsummen in Datenübertragungsprotokollen vergleichen. Bei Eingang der Daten an ihrem Zielort wird die Hashfunktion vom Empfänger berechnet. Wenn der Wert der vom Empfänger berechneten Hashfunktion mit dem des Absenders übereinstimmt, ist die Integrität der Nachricht gewährleistet.

Kryptografietypen

Im Wesentlichen werden zwei Kryptografietypen unterschieden:

- Kryptografie mit einem Geheimschlüssel
- Kryptografie mit einem öffentlichen Schlüssel

In kryptografischen Systemen bezieht sich der Begriff *Schlüssel* auf einen numerischen Wert, der von einem Algorithmus zum Ändern von Informationen verwendet wird, wodurch diese Informationen geschützt und nur für die Personen sichtbar sind, die über den entsprechenden Schlüssel zum Abfragen der Informationen verfügen.

Die **Kryptografie mit einem Geheimschlüssel** wird auch als *symmetrische Verschlüsselung* bezeichnet. Bei diesem Kryptografietyp kennen Absender und Empfänger denselben Geheimcode, den sogenannten *Schlüssel*. Das Verschlüsseln von Nachrichten auf Seiten des Absenders und das Entschlüsseln auf Seiten des Empfängers erfolgt mit demselben Schlüssel.

Dieses Verfahren eignet sich für die Datenübertragung bei einer begrenzten Personenzahl, ist allerdings für den Austausch von Geheimschlüsseln bei einer Vielzahl von Personen impraktikabel. Außerdem ist die sichere Mitteilung des Geheimschlüssels problematisch.

Bei der **Kryptografie mit einem öffentlichen Schlüssel**, der sogenannten *asymmetrischen Verschlüsselung*, wird ein Schlüsselpaar für die Verschlüsselung und Entschlüsselung verwendet. Dieses Kryptografieverfahren basiert auf Schlüsselpaaren, nämlich dem *öffentlichen* und dem *privaten* Schlüssel.

Der öffentliche Schlüssel kann ohne Gefährdung des privaten Schlüssels weitergeleitet werden; letzterer muss von seinem Eigentümer geheim gehalten werden. Da diese Schlüssel nur paarweise funktionieren, lässt sich die mit dem öffentlichen Schlüssel vorgenommene Verschlüsselung nur mit dem entsprechenden privaten Schlüssel entschlüsseln. Das folgende Beispiel veranschaulicht die Arbeitsweise des Kryptografieverfahrens mit einem öffentlichen Schlüssel:

- Frau Meier möchte geheime Informationen mit Herrn Müller austauschen. Frau Meier verschlüsselt ihre Nachricht mit dem öffentlichen Schlüssel von Herrn Müller (den Herr Müller öffentlich bekannt gegeben hat) und leitet die verschlüsselte Nachricht an Herrn Müller weiter.
- Wenn Herr Müller die Nachricht erhält, entschlüsselt er sie mit seinem privaten Schlüssel, damit er die Nachricht lesen kann.
- Wenn Herr Müller eine Antwort an Frau Meier sendet, verschlüsselt er die Nachricht mit dem öffentlichen Schlüssel von Frau Meier.
- Bei Eingang der Antwort von Herrn Müller entschlüsselt Frau Meier seine Nachricht mit ihrem privaten Schlüssel.

Der wesentliche Vorzug der asymmetrischen Verschlüsselung im Vergleich zur symmetrischen Verschlüsselung besteht darin, dass sich Absender und Empfänger keine Schlüssel im Voraus mitteilen müssen. Sofern der private Schlüssel geheim gehalten wird, ermöglichen öffentliche Schlüssel die Weiterleitung vertraulicher Informationen.

Kombinieren der Kryptografieverfahren mit öffentlichem und geheimen Schlüssel: Der größte Nachteil der Kryptografie mit einem öffentlichen Schlüssel besteht darin, dass die Verschlüsselung mit den in der PKI üblichen, sehr langen Schlüsseln bei den meisten Computersystemen zu Leistungsproblemen führen kann. Aus diesem Grund werden bei der Kryptografie häufig öffentliche und private Schlüssel kombiniert verwendet. Das folgende Beispiel veranschaulicht die Arbeitsweise:

- Herr Müller möchte geheime Informationen mit Frau Meier austauschen und erhält daher ihren öffentlichen Schlüssel. Außerdem erstellt er nur für diese Sitzung eine beliebige Ziffernfolge, auch *Sitzungsschlüssel* genannt.
- Herr Müller verwendet den öffentlichen Schlüssel von Frau Meier zum Chiffrieren des Sitzungsschlüssels.
- Herr Müller leitet die verschlüsselte Nachricht und den chiffrierten Sitzungsschlüssel an Frau Meier weiter.
- Frau Meier verwendet ihren privaten Schlüssel, um die Nachricht von Herrn Müller zu entschlüsseln und den Sitzungsschlüssel zu extrahieren.

Wenn Herr Müller und Frau Meier den Sitzungsschlüssel mit Erfolg austauschen, erübrigt sich die Kryptografie mit einem öffentlichen Schlüssel. Der Daten- und Informationsaustausch erfolgt dann nur auf Basis des Sitzungsschlüssels. Die Verschlüsselung mit einem öffentlichen Schlüssel wird beispielsweise zur Weiterleitung des geheimen Schlüssels verwendet. Beim Austausch des geheimen Schlüssels erfolgt die Datenübertragung durch Verschlüsselung mit dem geheimen Schlüssel.

Diese Lösung bietet die Vorzüge beider Verfahren, d. h. die Geschwindigkeit der Verschlüsselung mit einem geheimen Schlüssel und die Sicherheit der Verschlüsselung mit einem öffentlichen Schlüssel.

Digitale Zertifikate und Zertifizierungsstellen

Wie kann Frau Meier bei den oben beschriebenen Szenarien sicher sein, dass Herr Müller wirklich Herr Müller und kein Betrüger ist? Wenn Frau Meier ihren öffentlichen Schlüssel weiterleitet, muss auch Herr Müller sicher sein, dass Frau Meier tatsächlich die Person ist, die sie zu sein vorgibt.

Das ISO X.509-Protokoll definiert einen Mechanismus, ein sogenanntes *Zertifikat*, das den öffentlichen, von einer vertrauenswürdigen Organisation, einer *Zertifizierungsstelle*, signierten Schlüssel eines Benutzers enthält.

Zertifikate enthalten Informationen zum Festlegen von Identitäten in einem Netzwerk bei einem Prozess, der *Authentifizierung* genannt wird. Wie Führerscheine, Pässe oder sonstige Identitätsnachweise ermöglichen Zertifikate die gegenseitige Authentifizierung von Servern und Clients, bevor eine sichere Verbindung hergestellt wird.

Zertifikate sind nur für die Dauer eines bestimmten Zeitraums gültig. Bei Ablauf der Gültigkeitsdauer muss ein neues Zertifikat ausgestellt werden. Die Zertifizierungsstelle kann Zertifikate auch sperren.

Zur Herstellung einer SSL/TLS-Verbindung ist an einem Ende der Verbindung ein Serverzertifikat und am anderen Ende der Verbindung ein Stammzertifikat der Zertifizierungsstelle erforderlich, die das Serverzertifikat ausgestellt hat.

Serverzertifikat: Mit einem Serverzertifikat wird die Identität eines Servers bestätigt. Das für das Access Gateway erforderliche digitale Zertifikat wird *Serverzertifikat* genannt.

Stammzertifikat: Ein Stammzertifikat dient zur Identifizierung der Zertifizierungsstelle, die das Serverzertifikat signiert hat. Das Stammzertifikat gehört der Zertifizierungsstelle. Anhand dieses digitalen Zertifikats überprüft ein Clientgerät das Serverzertifikat.

Beim Herstellen einer SSL-Verbindung mit einem Webbrowser auf einem Clientgerät leitet der Server sein Zertifikat an den Client weiter.

Bei Eingang eines Serverzertifikats prüft der Webbrowser (z. B. Internet Explorer) auf dem Clientgerät, welche Zertifizierungsstelle das Zertifikat ausgestellt hat und ob diese Zertifizierungsstelle für den Client vertrauenswürdig ist. Wenn die Zertifizierungsstelle nicht vertrauenswürdig ist, fordert der Webbrowser den Benutzer auf, das Zertifikat zu akzeptieren oder abzulehnen (d. h. den Zugriff auf diese Website zu akzeptieren oder abzulehnen).

Wenn Frau Meier jetzt eine Nachricht von Herrn Müller erhält, wird anhand der lokal gespeicherten Informationen über die Zertifizierungsstelle geprüft, ob diese Zertifizierungsstelle das Zertifikat auch tatsächlich ausgestellt hat. Diese Informationen sind eine Kopie des eigenen Zertifikats der Zertifizierungsstelle und werden als *Stammzertifikat* bezeichnet.

In der Regel haben Zertifikate ein gemeinsames Format, das normalerweise auf ITU-Standards basiert. Zertifikate enthalten u. a. folgende Informationen:

Aussteller: Die Organisation, von der die Zertifikate ausgestellt werden.

Betreff: Die Identität, die durch das Zertifikat identifiziert wird.

Gültigkeitsdauer: Das Start- und Ablaufdatum eines Zertifikats.

Öffentlicher Schlüssel: Der zum Verschlüsseln der Daten verwendete öffentliche Schlüssel des Betreffs.

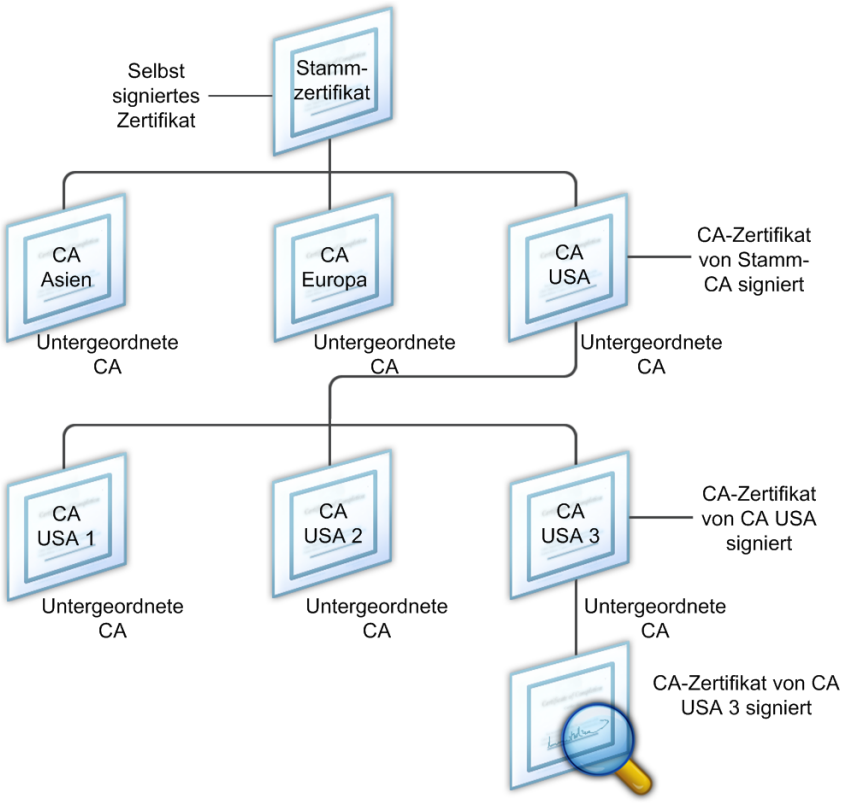
Signatur des Ausstellers: Die digitale Signatur der Zertifizierungsstelle für das Zertifikat, anhand dessen seine Authentizität gewährleistet wird.

Einige Unternehmen und Organisationen fungieren derzeit als Zertifizierungsstellen, u. a. VeriSign, Baltimore, Entrust und ihre jeweiligen verbundenen Unternehmen.

Zertifikatketten

Einige Organisationen delegieren die Ausstellung von Zertifikaten, um das mit der räumlichen Trennung zwischen Organisationseinheiten einhergehende Problem oder das Problem, das auf die Anwendung unterschiedlicher Ausstellungsrichtlinien für verschiedene Organisationsbereiche zurückzuführen ist, zu lösen.

Die Verantwortung für die Ausstellung von Zertifikaten kann durch die Einrichtung von untergeordneten Zertifizierungsstellen delegiert werden. Der X.509-Standard enthält ein Modell, mit dem sich eine Hierarchie von Zertifizierungsstellen (engl. Certificate Authority, CA) einrichten lässt. Bei diesem Modell befindet sich die Stammzertifizierungsstelle auf der obersten Hierarchieebene und hat ein selbst signiertes Zertifikat. Die der Stammzertifizierungsstelle direkt untergeordneten Zertifizierungsstellen lassen Zertifizierungsstellenzertifikate von der Stammzertifizierungsstelle signieren. Zertifizierungsstellen, die sich in der Hierarchie unter den untergeordneten Zertifizierungsstellen befinden, lassen ihre Zertifizierungsstellenzertifikate von den untergeordneten Zertifizierungsstellen signieren.



Hierarchische Struktur einer typischen digitalen Zertifikatkette

Zertifizierungsstellen können ihre eigenen Zertifikate signieren (d. h. sie sind selbst signiert) oder sie können auch von einer anderen Zertifizierungsstelle signiert werden. Selbst signierte Zertifikate stammen von sogenannten *Stamm-zertifizierungsstellen*. Nicht selbst signierte Zertifikate stammen von sogenannten *untergeordneten Zertifizierungsstellen* oder *Zwischenzertifizierungsstellen.*

Wenn ein Serverzertifikat von einer Zertifizierungsstelle mit einem selbst signierten Zertifikat signiert ist, besteht die Zertifikatkette aus genau zwei Zertifikaten: dem Zertifikat der Endeinheit und dem Zertifikat der Stammzertifizierungsstelle. Wenn ein Benutzer- oder Serverzertifikat von einer Zwischenzertifizierungsstelle signiert ist, ist die Zertifikatkette länger.

Die nachstehende Abbildung zeigt, dass die ersten beiden Elemente das Endeinheitszertifikat (in diesem Fall gwy01.firma.com) und das Zertifikat der Zwischenzertifizierungsstelle, und zwar in dieser Reihenfolge, sind. Nach dem Zertifikat der Zwischenzertifizierungsstelle folgt das Zertifikat ihrer Zertifizierungsstelle. Das letztgenannte Zertifikat in dieser Liste ist das Zertifikat der Stammzertifizierungsstelle. Jedes Zertifikat in der Kette bestätigt die Identität des vorhergehenden Zertifikats.

Typische Kette digitaler Zertifikate

Zertifikatsperrlisten

Gelegentlich veröffentlichen Zertifizierungsstellen Zertifikatsperrlisten. Zertifikatsperrlisten enthalten Informationen über nicht mehr vertrauenswürdige Zertifikate. Beispiel: Frau Meier verlässt das Unternehmen XYZ. Das Unternehmen kann das Zertifikat von Frau Meier auf eine Zertifikatsperrliste setzen, damit sie keine Nachrichten mehr mit diesem Schlüssel signieren kann.

Auf ähnliche Weise können Sie ein Zertifikat sperren, wenn ein privater Schlüssel öffentlich bekannt geworden ist oder wenn dieses Zertifikat abgelaufen und ein neues Zertifikat gültig ist. Bevor Sie einem öffentlichen Schlüssel trauen, sollten Sie sich vergewissern, dass das Zertifikat in keiner Zertifikatsperrliste aufgeführt ist.

Ablaufen und Erneuern von Zertifikaten

Zertifikate werden mit einer geplanten Lebensdauer (Gültigkeitsdauer) und einem ausdrücklichen Ablaufdatum ausgestellt. Nach dem Ausstellen werden Zertifikate bis zum Erreichen ihres Ablaufdatums als gültig angesehen. Nach dem Ablaufdatum kann ein Zertifikat nicht mehr zum Validieren einer Benutzersitzung verwendet werden. Diese Richtlinie dient zur Erhöhung der Sicherheit, da das Gefährdungspotenzial solcher Zertifikate eingeschränkt wird. Diese Ablaufdaten werden von der ausstellenden Zertifizierungsstelle festgelegt.

Normalerweise müssen Sie ein Zertifikat vor Erreichen seines Ablaufdatums erneuern. Die meisten Zertifizierungsstellen bieten einen gut dokumentierten Prozess für das Erneuern von Zertifikaten. Auf der Website Ihrer Zertifizierungsstelle finden Sie detaillierte Anweisungen zum Erneuern von Zertifikaten.

Beantragen von Zertifikaten

Beim Ermitteln der für Ihre Access Gateway-Bereitstellung erforderlichen Anzahl und Art von Zertifikaten müssen Sie entscheiden, bei welcher Stelle die Zertifikate zu beantragen sind. Diese Entscheidung hängt von mehreren Faktoren ab, wie u. a.:

- Ist Ihr Unternehmen eine Zertifizierungsstelle? Dies ist vermutlich nur bei sehr großen Unternehmen der Fall.
- Hat Ihr Unternehmen bereits Geschäftsbeziehungen zu einer öffentlichen Zertifizierungsstelle?
- Unterstützt das Windows-Betriebssystem mehrere öffentliche Zertifizierungsstellen?
- Zertifikatkosten, Ruf einer bestimmten öffentlichen Zertifizierungsstelle usw.

Ihr Unternehmen hat eine eigene Zertifizierungsstelle

Wenn Ihr Unternehmen eine eigene Zertifizierungsstelle hat, müssen Sie festlegen, ob es angemessen ist, Ihre unternehmenseigenen Zertifikate für die sichere Datenübertragung in Ihrer Access Gateway-Installation zu verwenden. Citrix empfiehlt, dass Sie sich mit Ihrer unternehmenseigenen Sicherheitsabteilung in Verbindung setzen, um diese Frage zu klären und nähere Anweisungen zu erhalten, wie Sie Zertifikate erhalten.

Wenn Sie nicht sicher sind, ob Ihr Unternehmen über eine eigene Zertifizierungsstelle verfügt, sollten Sie sich mit der Sicherheitsabteilung oder dem Sicherheitsexperten Ihres Unternehmens in Verbindung setzen.

Ihr Unternehmen hat keine eigene Zertifizierungsstelle

Wenn Ihr Unternehmen keine eigene Zertifizierungsstelle hat, müssen Sie Ihre Zertifikate bei einer öffentlichen Zertifizierungsstelle, wie beispielsweise VeriSign, beantragen.

Die Beantragung eines digitalen Zertifikats bei einer öffentlichen Zertifizierungsstelle schließt den folgenden Verifizierungsprozess ein:

- Auf Basis der von Ihrem Unternehmen vorgelegten Unternehmensinformationen kann die Zertifizierungsstelle die vermeintliche Identität Ihres Unternehmens überprüfen. Dabei können andere Unternehmensabteilungen in den Verifizierungsprozess eingebunden werden, wie beispielsweise die

Buchhaltung. Unter Umständen muss die Gründungsurkunde oder ein ähnliches Rechtsdokument vorgelegt werden.

- Personen mit der entsprechenden Bevollmächtigung in Ihrem Unternehmen müssen die von der Zertifizierungsstelle vorgelegten rechtsverbindlichen Vereinbarungen unterzeichnen.
- Da die Zertifizierungsstelle Ihr Unternehmen als Käufer prüft, ist die Einkaufsabteilung bei diesem Prozess vermutlich involviert.
- Sie legen der Zertifizierungsstelle die Kontaktinformationen der jeweiligen Ansprechpartner vor, die bei Fragen angerufen werden können.

Beantragen von Serverzertifikaten

Der Sicherheitsexperte Ihres Unternehmens sollte in der Lage sein, Serverzertifikate zu besorgen. Auf den Websites gängiger Zertifizierungsstellen, wie z. B. von VeriSign, finden Sie Anweisungen zum Erstellen von Serverzertifikaten mit verschiedenen Webserverprodukten. Weitere Informationen zum Erstellen einer Zertifikatsanforderung finden Sie unter „Erstellen und Installieren von Zertifikaten“ auf Seite 55.

Hinweis: Mehrere Zertifizierungsstellen bieten Testserverzertifikate für einen befristeten Zeitraum an. Es könnte sinnvoll sein, ein Testzertifikat zum Testen des Access Gateways zu beantragen, bevor es in einer Produktionsumgebung bereitgestellt wird. Dabei sollten Sie darauf achten, dass Sie die entsprechenden Teststammzertifikate herunterladen und auf jedem Clientgerät installieren, das eine Verbindung über das Access Gateway herstellt.

Digitale Zertifikate und deren Verwendung im Access Gateway

Das Access Gateway verwendet digitale Zertifikate zum Verschlüsseln und Authentifizieren von über eine Verbindung gesendetem Verkehr. Wenn das auf dem Access Gateway installierte digitale Zertifikat nicht von einer Zertifizierungsstelle signiert ist, wird der Verkehr zwar verschlüsselt, aber nicht authentifiziert. Die Authentifizierung des Verkehrs erfolgt nur, wenn das digitale Zertifikat von einer Zertifizierungsstelle signiert ist.

Wenn über eine Verbindung gesendeter Verkehr nicht authentifiziert wird, kann es bei der Verbindung zu „Man-in-the-Middle“-Angriffen kommen. Bei einem solchen Angriff fangen Dritte den öffentlichen Schlüssel ab, der vom Access Gateway an den Secure Access Client gesendet wird, und nutzen diesen, um das Access Gateway vorzutäuschen. Die Folge ist, dass der Benutzer, ohne es zu wissen, Authentifizierungsinformationen an den Angreifer sendet, der mit diesen Informationen eine Verbindung zum Access Gateway herstellen kann. Mit Zertifikaten, die von einer Zertifizierungsstelle signiert sind, werden solche Angriffe verhindert.

Wenn das auf dem Access Gateway installierte Zertifikat nicht von einer Zertifizierungsstelle signiert ist, wird Secure Access Client-Benutzern beider Anmeldung eine Sicherheitswarnung angezeigt.

Eine solche Sicherheitswarnung wird Secure Access Client-Benutzern so lange angezeigt, bis Sie ein von einer Zertifizierungsstelle signiertes Zertifikat auf dem Access Gateway und ein entsprechendes Zertifikat auf den Computern der Benutzer installiert haben. Benutzer können die Sicherheitswarnung im Dialogfeld mit den Verbindungseigenschaften auch deaktivieren.

Verwenden von Windows-Zertifikaten

Das Access Gateway enthält den Certificate Request Generator, mit dem automatisch eine Zertifikatsanforderung erstellt werden kann. Nachdem die Datei von der Zertifizierungsstelle zurückgesendet wurde, kann sie auf das Access Gateway hochgeladen werden. Die hochgeladene Datei wird automatisch in das korrekte Format umgewandelt.

Wenn Sie zum Erstellen des signierten Zertifikats nicht den Certificate Request Generator verwenden möchten, empfiehlt Citrix, für die Verwaltung von Zertifikatsaufgaben Win32 OpenSSL zu verwenden. Nähere Informationen zu Win32 Open SSL finden Sie auf der OpenSSL-Website unter http://www.openssl.org/. Binärdateien für Win32 Open SSL können von der Website http://www.openssl.org/related/binaries.html heruntergeladen werden.

Wenn Sie mit der Manipulation von Zertifikaten vertraut sind, können Sie auch Tools verwenden, um eine PEM-formatierte Datei zu erstellen. Das Zertifikat, das Sie auf das Access Gateway hochladen, muss die folgenden Eigenschaften haben:

- Das Zertifikat muss im PEM-Format vorliegen und einen privaten Schlüssel enthalten.
- Das signierte Zertifikat und der private Schlüssel müssen unverschlüsselt sein. Wenn zum Entschlüsseln ein Kennwort vorhanden ist, kann ein verschlüsselter öffentlicher Schlüssel verwendet werden.

Entschlüsseln des privaten Schlüssels

Führen Sie die hier genannten Schritte nur aus, wenn die Methode, die Sie zum Generieren des privaten Schlüssels verwenden, einen verschlüsselten Schlüssel zum Ergebnis hat.

So entschlüsseln Sie den privaten Schlüssel:

1. Geben Sie an der $-Eingabeaufforderung den folgenden Befehl ein: **openssl rsa**

   Wenn Sie diesen Befehl ohne Argumente eingeben, erhalten Sie folgende Aufforderung:

   ```
   read RSA key
   ```

2. Geben Sie den Namen des zu entschlüsselnden Kennworts ein.

   Wenn Sie den Namen des privaten Schlüssels und der entschlüsselten PEM-Datei kennen, können Sie auch den Befehl **openssl rsa** mit den zugehörigen Argumenten eingeben.

   Wenn der Dateiname des privaten Schlüssels z. B. **mein_schlüsseltag_schlüssel.pvk** und der entschlüsselte Dateiname **ausgabe_schlüssel.pem** lautet, geben Sie Folgendes ein: **openssl rsa -in mein_schlüsseltag_schlüssel.pvk -out ausgabe_schlüssel.pem**.

Weitere Informationen finden Sie auf der Open SSL-Website unter http://www.openssl.org/docs/apps/rsa.html#EXAMPLES.

Informationen zum Herunterladen von OpenSSL für Windows finden Sie auf der SourceForge-Website unter http://sourceforge.net/project/showfiles.php?group_id=23617&release_id=48801.

Umwandeln in ein PEM-formatiertes Zertifikat

Es ist möglich, dass das signierte Zertifikat, das Sie von der Zertifizierungsstelle erhalten, nicht das PEM-Format hat. Wenn die Datei im Binärformat (DER) vorliegt, wandeln Sie sie wie folgt in ein PEM-Format um:

openssl x509 -in *Zertifikatdatei* **-inform DER -outform PEM -out** *umgewandelteZertifikatdatei*

Wenn sich das Zertifikat bereits in einem Textformat befindet, könnte es sich um das PKCS-Format handeln. Zu PKCS-formatierten Zertifikaten kommt es, wenn Sie angeben, dass das Zertifikat in einem Microsoft- und nicht in einem Apache-Betriebssystem verwendet werden wird. Wenn das Zertifikat nicht im PEM-Format vorliegt, wird bei Eingabe des folgenden Befehls eine Fehlermeldung ausgegeben. *Zertifikatdatei* darf bei der Ausführung dieses Befehls nicht den privaten Schlüssel enthalten.

openssl verify -verbose -CApath /tmp *Zertifikatdatei*

Wenn dieser Befehl zur Ausgabe der folgenden Fehlermeldung führt, hat die Datei nicht das PEM-Format.

```
Zertifikatdatei: unable to load certificate file
4840:error:0906D064:PEM routines:PEM_read_bio:bad base64
decode:pem_lib.c:781:
```

So wandeln Sie das Zertifikat vom PKCS7- in das PEM-Format um:

1. Führen Sie den folgenden Befehl aus:

   openssl pkcs7 -in ./*Zertifikatdatei* **-print_certs**

   Das Ergebnis sieht in etwa wie folgt aus:

   ```
   subject=...
   ...
   -----BEGIN CERTIFICATE-----
   ... Server Certificate ...
   -----END CERTIFICATE-----

   subject=...
   ...
   -----BEGIN CERTIFICATE-----
   ... Intermediate Cert ...
   -----END CERTIFICATE-----
   ```

2. Kombinieren Sie die Serverzertifikatsdaten und die Zwischenzertifikatsdaten (sofern vorhanden) der Ausgabe mit dem privaten Schlüssel. Informationen hierzu finden Sie unter „Kombinieren des privaten Schlüssels mit dem signierten Zertifikat“ auf Seite 304 und „Generieren vertrauenswürdiger Zertifikate für mehrere Ebenen“ auf Seite 304.

Kombinieren des privaten Schlüssels mit dem signierten Zertifikat

Sie müssen das signierte Zertifikat mit dem privaten Schlüssel kombinieren. Erst dann können Sie es auf das Access Gateway hochladen.

So kombinieren Sie den privaten Schlüssel mit dem signierten Zertifikat:

1. Verwenden Sie einen Texteditor, um den unverschlüsselten privaten Schlüssel mit dem signierten Zertifikat im PEM-Dateiformat zu kombinieren.

   Der Dateiinhalt muss in etwa wie folgt aussehen:

   ```
   -----BEGIN RSA PRIVATE KEY-----
   <Unverschlüsselter privater Schlüssel>
   -----END RSA Private KEY-----
   -----BEGIN CERTIFICATE-----
   <Signiertes Zertifikat>
   -----END CERTIFICATE-----
   ```

2. Speichern Sie die PEM-Datei und geben Sie ihr dabei einen Namen, wie z. B. **AccessGateway.pem**.

Generieren vertrauenswürdiger Zertifikate für mehrere Ebenen

Sie müssen herausfinden, ob Ihr Zertifikat mehrere Ebenen hat und, falls dies zutrifft, die Zwischenzertifikate entsprechend handhaben.

Achtung: Alle Zertifikate für das Access Gateway, die mehr als eine Ebene haben, *müssen* sämtliche Zwischenzertifikate enthalten, da das System andernfalls unbrauchbar werden könnte.

So generieren Sie vertrauenswürdige Stammzertifikate für mehrere Ebenen:

1. Öffnen Sie den Internet Explorer und öffnen Sie über das Access Gateway eine Webadresse. Geben Sie z. B. eine Adresse wie die folgende ein:

   https://*IP-Adresse***:***httpPort***//www.***meineseite***.com**

   wobei gilt:

   IP-Adresse ist die IP-Adresse des Access Gateways.

   httpPort ist die Access Gateway-Portnummer.

2. Doppelklicken Sie auf das Schlosssymbol in der rechten unteren Ecke des Browsers.
3. Klicken Sie im Fenster *Zertifikat* auf die Registerkarte *Zertifizierungspfad*.
4. Doppelklicken Sie auf die erste Pfadebene, um die Zertifikatsinformationen für die erste Ebene aufzurufen, und klicken Sie auf die Registerkarte **Details**.
5. Klicken Sie unten auf die Schaltfläche **In Datei kopieren**.
6. Klicken Sie auf der ersten Seite des Zertifikatsexport-Assistenten auf **Weiter**.
7. Klicken Sie auf **Base-64-codiert** und anschließend auf **Weiter**.
8. Geben Sie einen Dateinamen ein, z. B. G:\tmp\servercert.cer. Überprüfen Sie die Informationen und notieren Sie sich den vollständigen Dateinamen. Klicken Sie auf **Fertig stellen**.
9. Klicken Sie auf **OK**, um das Fenster **Zertifikat** für die erste Ebene zu schließen.
10. Wiederholen Sie die Schritte 4 bis 10 für alle Ebenen außer der letzten Ebene.
11. Speichern Sie alle Zertifikate in einer Datei und stellen Sie sicher, dass sämtliche Zwischenzertifikate in der Zertifikatdatei enthalten sind, die Sie hochladen.

Die Datei zum Hochladen muss das folgende Format haben:

```
Privater Schlüssel
Serverzertifikat
Zwischenzertifikat 0
Zwischenzertifikat 1
Zwischenzertifikat 2
```

Anfordern von Zertifikaten für interne Verbindungen

Um die Sicherheit interner Verbindungen zu erhöhen, die vom Access Gateway ausgehen, können Sie festlegen, dass das Access Gateway die SSL-Serverzertifikate validieren muss. Das Überprüfen von SSL-Serverzertifikaten ist eine wichtige Sicherheitsmaßnahme, da so Sicherheitsverletzungen wie Man-in-the-Middle-Angriffe zu verhindert werden können.

Durch das Erzwingen der Überprüfung der SSL-Serverzertifikate erhöht sich die Sicherheit bei Verbindungen zwischen dem Access Gateway und den Servern, auf denen Access Gateway Advanced Edition ausgeführt wird. Diese Verbindungen sind sicherheitssensibel, weil sie zum Konfigurieren des Access Gateways und zum Gewähren oder Verweigern des Zugriffs auf Netzwerkressourcen unter Verwendung von Sitzungsrichtlinien verwendet werden.

Das Access Gateway setzt voraus, dass die richtigen Stammzertifikate installiert werden, die zum Signieren der Serverzertifikate verwendet werden. Weitere Informationen zu Stammzertifikaten finden Sie unter „Installieren von Stammzertifikaten auf dem Access Gateway“ auf Seite 60.

So legen Sie fest, dass für interne Clientverbindungen Serverzertifikate vorhanden sein müssen:

Aktivieren Sie auf der Registerkarte **Global Cluster Policies** unter **Select security options** die Option **Validate secure certificates for internal connections**.

Verwenden von Platzhalterzertifikaten

Das Access Gateway unterstützt die Validierung von Platzhalterzertifikaten für Secure Access Clients. Platzhalterzertifikate sind am Sternchen (*) in ihrem Namen erkennbar. Sie können eines der beiden folgenden Formate haben: **.meinefirma.com* oder *www*.meinefirma.com*. Bei Verwendung eines Platzhalterzertifikats können die Clients zwischen unterschiedlichen Webadressen wählen, z. B. http://www1.meinefirma.com oder http://www2.meinefirma.com. Durch die Verwendung eines Platzhalterzertifikats kann ein Zertifikat für mehrere Websites verwendet werden.

Beispiele für die Konfiguration des Netzwerkzugriffs

Nachdem Sie das Access Gateway installieren und für den Betrieb in Ihrer Netzwerkumgebung konfiguriert haben, können Sie den Benutzerzugriff auf die Server, Anwendungen und sonstigen Ressourcen im internen Netzwerk mit dem Administration Tool konfigurieren.

Das Konfigurieren des Benutzerzugriffs auf interne Netzwerkressourcen schließt die folgenden Schritte ein: Definieren zugänglicher Netzwerke für Split-Tunneling, Konfigurieren von Authentifizierung und Autorisierung, Erstellen von Benutzergruppen, Erstellen von lokalen Benutzern und Definieren der Zugriffssteuerungslisten für Benutzergruppen.

Hinweis: Eine Zugriffssteuerungsliste ist ein Richtliniensatz, mit der die Zugriffsstufe von Benutzern auf die Netzwerkressourcen festgelegt wird.

Das Access Gateway unterstützt verschiedene Authentifizierungs- und Autorisierungstypen, die sich in unterschiedlichen Kombinationen konfigurieren und mit Richtlinien verwenden lassen, um den Benutzerzugriff auf das interne Netzwerk zu steuern.

Aufgrund der Vielzahl von Optionen und Möglichkeiten bei der Konfiguration des Benutzerzugriffs auf das interne Netzwerk wird dieser Aspekt der Access Gateway-Konfiguration in vier verschiedenen Abschnitten dieses Handbuchs behandelt:

- Dieser Anhang enthält Beispielszenarien für den Benutzerzugriff und detaillierte Anweisungen, wie Sie das Access Gateway schrittweise zur Unterstützung der Zugriffsszenarios konfigurieren. Diese Szenarios sind keine Beispiele für echte Konfigurationen aus der Praxis, sondern vielmehr als eine Art Lernprogramm gedacht, damit Sie leichter verstehen, wie die im Administration Tool integrierten Funktionen zum Konfigurieren des Benutzerzugriffs zu verwenden sind.

Nachdem Sie sich mit diesen Beispielen und den Grundkenntnissen zum Konfigurieren des Benutzerzugriffs vertraut gemacht haben, können Sie den Benutzerzugriff auf das Access Gateway in Ihrer Produktionsumgebung anhand der in den folgenden Kapiteln enthaltenen Informationen konfigurieren:

- Kapitel 6, „Konfigurieren der Authentifizierung und Autorisierung“: In diesem Kapitel werden die verschiedenen Authentifizierungs- und Autorisierungsoptionen und deren Konfiguration erläutert.
- Kapitel 7, „Konfigurieren von Netzwerkzugriff und Gruppenressourcen“: In diesem Kapitel wird die Arbeit mit Benutzergruppen, Netzwerkressourcen und verschiedenen Richtlinien zum Definieren von Zugriffssteuerungslisten auf dem Access Gateway beschrieben.
- Kapitel 8, „Konfigurieren von Benutzerverbindungen für den Secure Access Client“: In diesem Kapitel werden Clientverbindungen zum Access Gateway beschrieben.

Konfigurationsbeispiele

Bevor Sie sich die Beispiele in diesem Kapitel durchlesen, sollten Sie sich mit den Einstellungen auf drei Registerkarten des Administration Tools vertraut machen. Mit den Einstellungen auf diesen Registerkarten wird der Benutzerzugriff auf interne Netzwerkressourcen gesteuert:

- Global Cluster Policies
- Authentication
- Access Policy Manager

Nachstehend finden Sie eine Liste der in diesem Kapitel beschriebenen Konfigurationsbeispiele für den Benutzerzugriff.

- Konfigurieren der LDAP-Authentifizierung und -Autorisierung: Bei diesem Beispiel wird schrittweise erläutert, wie ein Administrator den Zugriff auf interne Netzwerkressourcen in einer LDAP-Umgebung gewähren könnte.
- Erstellen von Gastkonten mit der Liste **Local Users**: In diesem Beispiel wird das Szenario für das Konfigurieren der LDAP-Authentifizierung und -Autorisierung erweitert, um das Konzept der lokalen Benutzer zu erläutern.
- Konfigurieren der lokalen Autorisierung: In diesem Beispiel wird das Konzept der lokalen Autorisierung erläutert, indem die im Szenario für das Erstellen von Gastkonten beschriebene Konfiguration mit der Liste **Local Users** geringfügig geändert wird.

Konfigurieren der LDAP-Authentifizierung und -Autorisierung:

Dieses Beispiel veranschaulicht, wie ein Administrator mit den Einstellungen im Administration Tool den Benutzerzugriff konfigurieren könnte:

- Das Unternehmen verwendet nur ein LDAP-Verzeichnis als Benutzerrepository.
- Remotebenutzer, die für die Vertriebsabteilung arbeiten, müssen Zugriff auf einen E-Mail-Server, einen Webkonferenzserver, eine Webanwendung für den Vertrieb und mehrere Dateiserver im internen Netzwerk haben.
- Remotebenutzer, die für die technische Abteilung arbeiten, müssen Zugriff auf einen E-Mail-Server, einen Webkonferenzserver und mehrere Dateiserver im internen Netzwerk haben.
- Im internen Netzwerk sind zwar drei E-Mail-Server vorhanden; der Administrator möchte Remotebenutzern jedoch nur den Zugriff auf einen dieser E-Mail-Server gewähren.

Um den Zugriff auf die internen Netzwerkressourcen in diesem Szenario zu konfigurieren, führt der Administrator diese beiden grundlegenden Arbeitsschritte aus:

- Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung
- Konfigurieren des Access Gateways zur Unterstützung des Zugriffs auf die internen Netzwerkressourcen

Diese Arbeitsschritte werden im Folgenden jeweils näher erläutert.

Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung

Die Vorbereitung der Konfiguration von LDAP-Authentifizierung und -Autorisierung ist der erste Arbeitsschritt, den der Administrator beim Szenario für das Konfigurieren der LDAP-Authentifizierung und -Autorisierung vom ausführt.

Bei diesem Arbeitsschritt stellt der Administrator die Informationen zusammen, die für die Konfiguration des Access Gateways zur Unterstützung von LDAP-Authentifizierung und -Autorisierung erforderlich sind.

Dabei sind die folgenden Arbeitsschritte erforderlich:

- Festlegen, welche internen Netzwerke die jeweils gewünschten Ressourcen enthalten
- Festlegen, welche Benutzer aus den Abteilungen Vertrieb und Technik Remotezugriff benötigen
- Sammeln der LDAP-Verzeichnisinformationen

Festlegen, welche internen Netzwerke die gewünschten Ressourcen enthalten

Zum Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung muss der Administrator zuerst festlegen, welche internen Netzwerke die gewünschten Ressourcen enthalten.

Dabei legt der Administrator die Netzwerkpfade der Ressourcen fest, auf die Remotebenutzer Zugriff haben müssen. Im Folgenden werden noch einmal die Anforderungen wiederholt:

- Remotebenutzer, die für die Vertriebsabteilung arbeiten, müssen Zugriff auf einen E-Mail-Server, einen Webkonferenzserver, eine Webanwendung für den Vertrieb und mehrere Dateiserver im internen Netzwerk haben.
- Remotebenutzer, die für die technische Abteilung arbeiten, müssen Zugriff auf einen E-Mail-Server, einen Webkonferenzserver und mehrere Dateiserver im internen Netzwerk haben.
- Im internen Netzwerk sind zwar drei E-Mail-Server vorhanden; der Administrator möchte Remotebenutzern jedoch nur den Zugriff auf einen dieser E-Mail-Server gewähren.

Für diesen Arbeitsschritt wird angenommen, dass der Administrator die folgenden Informationen gesammelt hat:

- Der Webkonferenzserver, die E-Mail-Server und die Dateiserver, auf die Remotebenutzer aus den Abteilungen Vertrieb und Technik zugreifen müssen, befinden sich im Netzwerk 10.10.0.0/24.
- Der Server, auf dem die Webanwendung für den Vertrieb installiert ist, befindet sich im Netzwerk 10.60.10.0/24.
- Der einzelne E-Mail-Server, auf den Remotebenutzer zugreifen müssen, hat die IP-Adresse 10.10.25.50.

Festlegen, welche Benutzer aus den Abteilungen Vertrieb und Technik Remotezugriff benötigen

Zum Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung muss der Administrator im zweiten Arbeitsschritt festlegen, welche Benutzer aus den Abteilungen Vertrieb und Technik Remotezugriff benötigen.

Bevor ein Administrator das Access Gateway zur Unterstützung der Autorisierung mit einem LDAP-Verzeichnis konfigurieren kann, muss er verstehen, wie das Access Gateway den Autorisierungsvorgang mit Gruppen vornimmt.

Insbesondere muss der Administrator das Verhältnis zwischen der Gruppenmitgliedschaft eines Benutzers im LDAP-Verzeichnis und der Gruppenmitgliedschaft eines Benutzers auf dem Access Gateway verstehen.

Hinweis: Zur Unterstützung von Autorisierungstypen basiert das Access Gateway ähnlich wie RADIUS auf Benutzergruppen.

Wenn ein Benutzer in einem LDAP-Verzeichnis eine Verbindung zum Access Gateway herstellt, läuft die grundlegende Authentifizierung und Autorisierung in der folgenden Reihenfolge ab:

- Nachdem ein Benutzer seine Authentifizierungsinformationen vom LDAP-Verzeichnis eingegeben hat, sucht das Access Gateway nach diesem Benutzer im LDAP-Verzeichnis, überprüft die Anmeldeinformationen des Benutzers und meldet den Benutzer an.
- Nach der erfolgreichen Authentifizierung prüft das Access Gateway ein Attribut im Personeneintrag des LDAP-Verzeichnisses des Benutzers, um festzustellen, welchen LDAP-Verzeichnisgruppen dieser Benutzer angehört.

  Wenn das Access Gateway beispielsweise mit Microsoft Active Directory arbeitet, prüft das Access Gateway das Attribut „memberOf" im Personeneintrag, um festzustellen, welchen Gruppen ein Benutzer angehört.

  In diesem Beispiel wird angenommen, dass der Benutzer Mitglied einer LDAP-Verzeichnisgruppe namens „Vertriebsaußendienst" ist.

- Dann sucht das Access Gateway nach einer auf der Registerkarte **Access Policy Manager** im Administration Tool konfigurierten Benutzergruppe, deren Name mit dem Namen einer LDAP-Verzeichnisgruppe übereinstimmt, der dieser Benutzer angehört.

  In diesem Beispiel sucht das Access Gateway nach einer auf dem Access Gateway konfigurierten Benutzergruppe namens „Vertriebsaußendienst“.

  Wenn das Access Gateway eine solche Benutzergruppe findet, erhält der Benutzer die der Benutzergruppe auf dem Access Gateway zugewiesenen Zugriffsberechtigungen (Autorisierung).

  In diesem Beispiel gewährt das Access Gateway dem Benutzer die Zugriffsstufen, die mit der Benutzergruppe „Vertriebsaußendienst“ auf der Registerkarte **Access Policy Manager** im Administration Tool verknüpft sind.

Bevor der Administrator den Benutzern aus den Abteilungen Vertrieb und Technik den Zugriff auf interne Netzwerkressourcen über das Access Gateway gewähren kann, muss er also wissen, welchen LDAP-Verzeichnisgruppen diese Benutzer angehören. Jetzt muss der Administrator in diesem Szenario einen der beiden Schritte in Bezug auf die Gruppenmitgliedschaft der Benutzer ausführen:

- Er muss die Gruppen im LDAP-Verzeichnis identifizieren, die sämtliche Mitglieder enthalten, für die Remotezugriff auf die internen Netzwerke erforderlich ist.
- Wenn keine Gruppe vorhanden ist, die alle betreffenden Mitglieder enthält, kann der Administrator neue Gruppen im LDAP-Verzeichnis erstellen und die betreffenden Mitglieder diesen Gruppen hinzufügen.

In diesem Beispiel wird davon ausgegangen, dass der Administrator Gruppen namens „Vertriebsaußendienst“ und „Außendiensttechniker“ im LDAP-Verzeichnis erstellt und diesen Gruppen Benutzer aus den Abteilungen Vertrieb und Technik hinzufügt, die Remotezugriff auf die internen Netzwerkressourcen haben sollen.

Sammeln der LDAP-Verzeichnisinformationen

Zum Vorbereiten der Konfiguration von LDAP-Authentifizierung und -Autorisierung muss der Administrator als letzten Schritt die LDAP-Verzeichnisinformationen sammeln.

In diesem Beispiel verwendet das Unternehmen nur ein LDAP-Verzeichnis als Benutzerrepository.

Bevor der Administrator das Access Gateway für die Unterstützung von Authentifizierung und Autorisierung mit einem LDAP-Verzeichnis konfigurieren kann, muss er Informationen über das LDAP-Verzeichnis sammeln. Mit diesen Informationen wird das Access Gateway später zum Herstellen einer Verbindung zum LDAP-Verzeichnis konfiguriert, um nach Benutzer- und Gruppennamen zu suchen.

Hinweis: Welche Informationen zum Konfigurieren eines bestimmten Authentifizierungs- oder Autorisierungstyps erforderlich sind, finden Sie in der *Access Gateway Standard Edition Installationscheckliste*. Sie können auch im Administrator Tool auf die Registerkarte **Authentication** klicken und einen Testauthentifizierungsbereich erstellen, der die Authentifizierungs- und Autorisierungstypen enthält, die unterstützt werden müssen. Sammeln Sie die erforderlichen Informationen, um die Felder für die gewählten Authentifizierungs- und Autorisierungstypen auszufüllen.

In diesem Arbeitsschritt sammelt der Administrator die folgenden Informationen über das LDAP-Verzeichnis.

- **IP-Adresse des LDAP-Servers:** Die IP-Adresse des Computers, auf dem der LDAP-Server ausgeführt wird.
- **LDAP-Serverport:** Der Port, auf dem der LDAP-Server Verbindungen abhört. Der Standardport für LDAP-Verbindungen ist Port 389.
- **LDAP-Administrator-DN und LDAP-Administratorkennwort:** Wenn für den Zugriff von Anwendungen auf das LDAP-Verzeichnis eine Authentifizierung erforderlich ist, muss der Administrator den Namen des Benutzerkontos, mit dem das Access Gateway diese Authentifizierung vornehmen soll, sowie das mit diesem Konto verknüpfte Kennwort kennen.

- **LDAP-Basis-DN:** Das Basisobjekt des Verzeichnisses (oder die Verzeichnisebene), in dem Benutzernamen gespeichert werden. Auf dieser Verzeichnisebene müssen alle Remotebenutzer einen Personeneintrag haben. Nachstehend einige Beispielwerte:

  ou=Benutzer,dc=ace,dc=com

  cn=Benutzer,dc=ace,dc=com

- **LDAP-Attribut für Serveranmeldung:** Das Attribut eines Personeneintrags im LDAP-Verzeichnis, das einen Benutzernamen enthält. Die folgende Tabelle enthält Beispiele für die Benutzernamen-Attributfelder für verschiedene LDAP-Verzeichnisse:

LDAP-Server	Benutzerattribut	Groß-/Kleinschreibung relevant
Microsoft Active Directory-Server	sAMAccountName	Nein
Novell eDirectory	cn	Ja
IBM Directory Server	uid	
Lotus Domino	CN	
Sun ONE-Verzeichnis (früher iPlanet)	uid oder cn	Ja

- **LDAP-Gruppenattribut:** Das Attribut des Personeneintrag eines Benutzers, das eine Liste der Gruppen enthält, denen dieser Benutzer angehört, z. B. „memberOf“. Das LDAP-Gruppenattribut wird nur bei der LDAP-Autorisierung verwendet.

Jetzt hat der Administrator alle notwendigen Vorbereitungsschritte für die Konfiguration der LDAP-Authentifizierung und -Autorisierung abgeschlossen. Danach stehen dem Administrator die folgenden Informationen zur Verfügung:

- Die exakten Netzwerkpfade aller Netzwerkressourcen, auf die Remotebenutzer aus den Abteilungen Vertrieb und Technik zugreifen müssen.
- Die Namen der Benutzergruppen im LDAP-Verzeichnis mit den Benutzern aus den Abteilungen Vertrieb und Technik, die Remotezugriff benötigen (bei diesem Beispiel „Vertriebsaußendienst“ und „Außendiensttechniker“)
- Die exakten LDAP-Verzeichnisinformationen, die zum Konfigurieren des Access Gateways für die Arbeit mit dem LDAP-Verzeichnis erforderlich sind.

Anhand dieser Informationen kann der Administrator nun das Access Gateway konfigurieren, um den Benutzern aus den Abteilungen Vertrieb und Technik Zugriff auf die internen Netzwerkressourcen zu gewähren.

Konfigurieren des Access Gateways zur Unterstützung des Zugriffs auf die internen Netzwerkressourcen

Die Konfiguration des Access Gateways zur Unterstützung des Zugriffs auf die internen Netzwerkressourcen ist der letzte Arbeitsschritt, den der Administrator bei der Konfiguration der LDAP-Authentifizierung und -Autorisierung ausführt.

Dabei verwendet der Administrator die im vorigen Arbeitsschritt gesammelten Informationen, um die Einstellungen im Administration Tool zu konfigurieren, damit Remotebenutzer auf die internen Netzwerkressourcen zugreifen können.

Dabei sind die folgenden fünf Arbeitsschritte erforderlich:

- Konfigurieren der zugänglichen Netzwerke
- Erstellen eines LDAP-Authentifizierungsbereichs
- Erstellen der entsprechenden Gruppen auf dem Access Gateway
- Erstellen und Zuweisen von Netzwerkressourcen für die Benutzergruppen
- Erstellen einer Anwendungsrichtlinie für den E-Mail-Server

Diese Schritte werden im Folgenden genauer erläutert.

Konfigurieren der zugänglichen Netzwerke

Das Konfigurieren der zugänglichen Netzwerke ist der erste von fünf Arbeitsschritten, die der Administrator ausführt, um beim Konfigurationsszenario für die LDAP-Authentifizierung und -Autorisierung den Zugriff auf die internen Netzwerkressourcen zu konfigurieren.

In diesem Arbeitsschritt gibt der Administrator die internen Netzwerke mit den Netzwerkressourcen an, auf die Benutzer über den Secure Access Client zugreifen müssen.

Im vorigen Arbeitsschritt hat der Administrator festgelegt, dass Remotebenutzer aus den Abteilungen Vertrieb und Technik auf die in die Ressourcen in folgenden internen Netzwerken Zugriff haben müssen:

- Webkonferenzserver, Dateiserver und E-Mail-Server in Netzwerk 10.10.0.0/24
- Server mit der Webanwendung für den Vertrieb in Netzwerk 10.60.10.0/24

Der Administrator legt diese Netzwerke als zugängliche Netzwerke fest. Durch die Angabe der zugänglichen Netzwerke kann der Secure Access Client Split-Tunneling unterstützen.

Wenn sich ein Benutzer am Access Gateway anmeldet, leitet das Access Gateway diese Netzwerkliste an den Secure Access Client auf dem Computer des Benutzers weiter. Der Secure Access Client verwendet die Liste als Filter, um festzulegen, welche ausgehenden Pakete an das Access Gateway und welche Pakete anderweitig weitergeleitet werden sollen. Der Secure Access Client leitet nur die für das Access Gateway bestimmten Pakete über den sicheren Tunnel an das Access Gateway weiter.

Hinweis: Wenn Split-Tunneling nicht unterstützt werden soll, erübrigt sich das Konfigurieren der zugänglichen Netzwerke.

So konfigurieren Sie zugängliche Netzwerke:

1. Öffnen Sie das Administration Tool.
2. Klicken Sie auf die Registerkarte **Global Cluster Policies**.
3. Aktivieren Sie bei Bedarf die Option **Enable split tunneling**.
4. Geben Sie im Feld **Accessible networks** alle internen Netzwerke ein, auf die das Access Gateway zugreifen muss. Trennen Sie die einzelnen Netzwerkeinträge durch ein Leerzeichen oder einen Zeilenumbruch voneinander. Bei diesem Zugriffsszenario würde der Administrator die folgenden Eingaben machen:

   10.10.0.0/24

   10.60.10.0/24
5. Aktivieren Sie das Kontrollkästchen **Enable logon page authentication**. Bei dieser Einstellung müssen sich die Benutzer authentifizieren, wenn sie über einen Webbrowser auf die Portalseite des Access Gateways zugreifen.
6. Zur Vereinfachung dieses Beispiels wird angenommen, dass der Administrator alle anderen Kontrollkästchen auf der Registerkarte **Global Cluster Policies** deaktiviert. Weitere Informationen über Split-Tunneling finden Sie unter „Aktivieren von Split-Tunneling und zugänglichen Netzwerken“ auf Seite 116. Weitere Informationen über die Einstellung **Deny Access without access control list** finden Sie unter „Zugriffssteuerungslisten“ auf Seite 92.

Erstellen eines LDAP-Authentifizierungs- und Autorisierungsbereichs

Das Erstellen eines LDAP-Authentifizierungs- und -Autorisierungsbereichs ist der zweite von fünf Arbeitsschritten, die der Administrator zum Konfigurieren des Zugriffs auf die internen Netzwerkressourcen ausführt.

In diesem Szenario sind alle Benutzer aus den Abteilungen Vertrieb und Technik in einem unternehmensinternen LDAP-Verzeichnis aufgeführt.

Zum Authentifizieren der in einem LDAP-Verzeichnis aufgeführten Benutzer muss der Administrator einen Authentifizierungsbereich erstellen, der die LDAP-Authentifizierung unterstützt.

Um den in LDAP-Verzeichnisgruppen aufgeführten Benutzern Zugriff auf die internen Netzwerkressourcen zu gestatten, wählt der Administrator die LDAP-Authentifizierung als Autorisierungstyp für den Bereich aus.

Da sich Benutzer über das LDAP-Verzeichnis authentifizieren, richtet der Administrator den Authentifizierungsbereich **Default** als Standardbereich zur Unterstützung der LDAP-Authentifizierung und -Autorisierung ein.

Zum Einrichten des Standardbereichs zur Unterstützung der LDAP-Authentifizierung löscht der Administrator zuerst den vorhandenen Standardbereich (**Default**) und erstellt dann sofort einen neuen Standardbereich, der LDAP-Authentifizierung unterstützt. Dieser neue Bereich enthält die Adresse, den Port und andere LDAP-Verzeichnisinformationen, die das Access Gateway zum Herstellen einer Verbindung zum LDAP-Verzeichnisserver und zum Suchen nach Namen im Verzeichnis benötigt.

Hinweis: Der auf dem Access Gateway vorhandene Standardbereich wird für die lokale Authentifizierung konfiguriert. Durch das Löschen des vorhandenen Standardbereichs und das Erstellen eines neuen Standardbereichs für LDAP erleichtert der Administrator den Anmeldevorgang für den Endbenutzer. Benutzer, die sich über den Standardbereich authentifizieren, müssen den Bereichsnamen nicht als Bestandteil ihrer Anmeldeinformationen eingeben. Weitere Informationen zu Bereichen, Authentifizierung und Autorisierung finden Sie unter „Sichern von Verbindungen mit Authentifizierung und Autorisierung“ auf Seite 57.

Zur Ausführung dieses Arbeitsschritts muss der Administrator die im vorigen Arbeitsschritt „Sammeln der LDAP-Verzeichnisinformationen“ gesammelten Informationen griffbereit haben.

So löschen Sie den vorhandenen Standardbereich (Default) und erstellen einen neuen Standardbereich, der LDAP-Authentifizierung und -Autorisierung unterstützt:

1. Klicken Sie im Access Gateway Administration Tool auf die Registerkarte **Authentication**.
2. Öffnen Sie das Fenster für den Bereich **Default**.
3. Wählen Sie im Menü **Action** den Befehl **Remove "Default" realm**.

   Es wird eine Warnmeldung angezeigt.
4. Klicken Sie auf **Ja**.
5. Geben Sie im Feld **Realm name** den Namen **Default** ein.
6. Wählen Sie **One Source** und klicken Sie auf **Add**.
7. Aktivieren Sie im Dialogfeld **Select Authentication Type** die Option **LDAP authentication** und klicken Sie dann auf **OK**.

   Dann wird das Fenster für den neuen Standardbereich geöffnet.
8. Füllen Sie im Fenster für den neuen Standardbereich auf der Registerkarte **Authentication** die erforderlichen Felder aus, um dem Access Gateway Zugriff auf den LDAP-Server zu ermöglichen. (Verwenden Sie hierfür die im vorigen Arbeitsschritt „Sammeln der LDAP-Verzeichnisinformationen" gesammelten Informationen.)
9. Klicken Sie auf die Registerkarte **Authorization**.
10. Wählen Sie unter **Authorization type** die Option **LDAP authorization**.
11. Füllen Sie auf der Registerkarte **Authorization** die erforderlichen Felder aus, um dem Access Gateway Zugriff auf den LDAP-Server zu ermöglichen.
12. Klicken Sie auf **Submit**.

Weitere Informationen zum Erstellen von Bereichen finden Sie unter „Arbeiten mit Bereichen" auf Seite 61.

Erstellen der entsprechenden Gruppen auf dem Access Gateway

Das Erstellen der entsprechenden Gruppen auf dem Access Gateway ist der dritte von fünf Arbeitsschritten, die der Administrator ausführt, um beim Konfigurationsszenario für die LDAP-Authentifizierung und -Autorisierung den Zugriff auf die internen Netzwerkressourcen zu konfigurieren.

In diesem Schritt erstellt der Administrator Benutzergruppen auf dem Access Gateway, deren Namen mit den Namen der Gruppen übereinstimmen, die der Administrator im LDAP-Verzeichnis gefunden oder erstellt hat.

In einem vorigen Arbeitsschritt hat der Administrator die LDAP-Verzeichnisgruppen „Vertriebsaußendienst“ und „Außendiensttechniker“ im LDAP-Verzeichnis erstellt.

In diesem Schritt muss der Administrator nun Benutzergruppen namens „Vertriebsaußendienst“ und „Außendiensttechniker“ auf dem Access Gateway erstellen.

So erstellen Sie Benutzergruppen auf dem Access Gateway:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **User Groups** und klicken Sie dann auf **New Group**.

   Geben Sie im Feld **Group Name** einen Namen ein, dessen Schreibweise (Groß- und Kleinschreibung) genau mit dem Namen einer LDAP-Verzeichnisgruppe aus dem vorigen Schritt übereinstimmt.

   Geben Sie beispielsweise „Vertriebsaußendienst“ ein und klicken Sie dann auf **OK**.
3. Jetzt wird das Eigenschaften-Dialogfeld der Gruppe angezeigt. Es enthält mehrere Registerkarten. Zur Vereinfachung dieses Beispiels akzeptieren Sie alle Standardeinstellungen für die Gruppeneigenschaften und klicken Sie auf **OK**.

   Die Gruppeneigenschaften enthalten zusätzliche Einstellungen, die sich auf den Benutzerzugriff auswirken. Weitere Informationen zu Gruppeneigenschaften und zum Erstellen von lokalen Gruppen finden Sie unter „Konfigurieren von Benutzergruppen“ auf Seite 117.

Erstellen und Zuweisen von Netzwerkressourcen für die Benutzergruppen

Das Erstellen und Zuweisen von Netzwerkressourcen für die Benutzergruppen ist der vierte von fünf Arbeitsschritten, die der Administrator ausführt, um beim Konfigurationsszenario für die LDAP-Authentifizierung und -Autorisierung den Zugriff auf die internen Netzwerkressourcen zu konfigurieren.

In diesem Schritt gibt der Administrator an, auf welche Netzwerkressourcen (Netzwerksegmente oder einzelne Computer) Benutzer zugreifen dürfen, und weist diese Ressourcen dann den Benutzergruppen auf dem Access Gateway zu.

Dabei führt der Administrator folgende Schritte aus:

- Erstellen einer Netzwerkressource namens „Vertriebsressource“ und Zuweisen dieser Ressource zur Benutzergruppe „Vertriebsaußendienst“
- Erstellen einer Netzwerkressource namens „Technische Ressource“ und Zuweisen dieser Ressource zur Benutzergruppe „Außendiensttechniker“

Erstellen und Zuweisen von Netzwerkressourcen für die Benutzer im Vertrieb

In diesem Abschnitt wird kurz erläutert, wie der Administrator eine Netzwerkressource für die Benutzer im Vertrieb erstellt und diesen Benutzern zuweist.

Wie bereits oben erwähnt, benötigen die Benutzer im Vertrieb Zugriff auf die folgenden Systeme:

- E-Mail-Server, Webkonferenzserver und mehrere Dateiserver im Netzwerk 10.10.0.0/24
- Webanwendung für den Vertrieb im Netzwerk 10.60.10.0/24

So erstellen Sie eine Netzwerkressource namens „Vertriebsressource“ für die Benutzer im Vertrieb:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste im linken Bereich auf **Network Resources** und klicken Sie dann auf **New Network Resource**.
3. Geben Sie „Vertriebsressource“ als Namen für die Netzwerkressource ein und klicken Sie auf **OK**.
4. Geben Sie im Feld **Network and subnet mask** die beiden IP-Adress-/Subnetzpaare für die Ressourcen ein. Trennen Sie diese IP-Adress-/Subnetzpaare jeweils durch ein Leerzeichen voneinander:

   10.10.0.0/24 10.60.10.0/24
5. Zur Vereinfachung dieses Beispiels übernimmt der Administrator die Standardwerte für die anderen Einstellungen im Eigenschaften-Dialogfeld der Netzwerkressource und klickt auf **OK**.

Nach dem Erstellen dieser Netzwerkressource geht der Administrator wie nachstehend beschrieben vor, um diese Netzwerkressource der Zugriffssteuerungsliste für die Benutzergruppe „Vertriebsaußendienst“ hinzuzufügen.

1. Klicken Sie im Access Gateway Administration Tool auf die Registerkarte **Access Policy Manager**.
2. Erweitern Sie im linken Bereich den Eintrag **User Groups** und dann die Benutzergruppe „Vertriebsaußendienst“.

3. Erweitern Sie im rechten Bereich den Eintrag **Network Resources**.
4. Klicken Sie auf die Netzwerkressource „Vertriebsressource“ und ziehen Sie diese im linken Bereich auf den Knoten **Network Policies** unter der Benutzergruppe „Vertriebsaußendienst“.

   Hierdurch gewährt der Administrator den mit dieser Benutzergruppe verknüpften Benutzern Zugriff auf die Systeme, die in der Netzwerkressource „Vertriebsressource“ definiert sind.

Hinweis: Im obigen Arbeitsschritt hat der Administrator die Netzwerkressource „Vertriebsressource“ der Zugriffssteuerungsliste der Benutzergruppe „Vertriebsaußendienst“ zugewiesen. Zugriffssteuerungslisten werden vom Administrator auf dem Access Gateway durch Hinzufügen der mit der Benutzergruppe verknüpften Netzwerk-, Anwendungs-, Kiosk- und Endpunktrichtlinien erstellt. Die Zugriffssteuerungsliste besteht aus allen Richtlinien, die einer Benutzergruppe auf dem Access Gateway zugewiesen sind.

Erstellen und Zuweisen von Netzwerkressourcen für die Benutzer im Bereich Technik

In diesem Abschnitt wird kurz erläutert, wie der Administrator eine Netzwerkressource für die Benutzer im Bereich Technik erstellt und diesen Benutzern zuweist. Abgesehen davon, dass der Administrator den Benutzern im Bereich Technik keinen Zugriff auf die Webanwendung für den Vertrieb in Netzwerk 10.60.10.0/24 gewährt, ist die Vorgehensweise im Wesentlichen identisch mit dem vorigen Arbeitsschritt für die Benutzer im Vertrieb.

Wie bereits oben erwähnt, müssen die Techniker auf einen Webkonferenzserver, einen E-Mail-Server und mehrere Dateiserver zugreifen. Alle diese Server befinden sich im Netzwerk 10.10.0.0/24.

So gewähren Sie den Benutzern aus dem Bereich Technik Zugriff auf das Netzwerk:

1. Erstellen Sie im rechten Bereich der Registerkarte **Access Policy Manager** im Access Gateway Administration Tool eine neue Netzwerkressource namens „Technikerressourcen“. Geben Sie beim Erstellen dieser Ressource nur das Netzwerk 10.10.0.0/24 an.
2. Erweitern Sie im linken Bereich die Benutzergruppe „Außendiensttechniker“.
3. Ziehen Sie die Netzwerkressource „Technikerressourcen“ aus dem rechten Bereich der Registerkarte **Access Policy Manager** auf **Network Policies** der Gruppe „Außendiensttechniker“ im linken Bereich.

Jetzt ist die Netzwerkressource „Technikerressourcen“ ein Bestandteil der Zugriffssteuerungsliste für die Gruppe „Außendiensttechniker“.

Hinweis: In komplexeren Umgebungen muss der Zugriff u. U. auf ein bestimmtes Segment eines größeren Netzwerks eingeschränkt werden. Beispiel: Ein Administrator muss den Zugriff auf das Netzwerk 10.0.20.x verweigern, doch den Zugriff auf alles andere im Netzwerk 10.0.x.x zulassen. Der Administrator erstellt eine Netzwerkressource für das Netzwerk 10.0.20.x und eine Netzwerkressource für das Netzwerk 10.0.x.x und weist der Benutzergruppe beide Netzwerkressourcen zu. Dann klickt der Administrator jeweils mit der rechten Maustaste auf die beiden Ressourcen, um den Zugriff auf die Ressource im Netzwerk 10.0.20.x zu verweigern und den Zugriff auf die Ressource im Netzwerk 10.0.x.x zuzulassen.

In solchen Fällen konfigurieren Sie zuerst die Richtlinie, wonach der Zugriff auf 10.0.20.x verweigert wird, und dann die Richtlinie, wonach der Zugriff auf das Netzwerk 10.0.x.x zugelassen wird. Konfigurieren Sie die Richtlinie mit den größten Einschränkungen stets zuerst und die Richtlinie mit den geringsten Einschränkungen zuletzt.

Erstellen einer Anwendungsrichtlinie für einen E-Mail-Server

Das Erstellen einer Anwendungsrichtlinie für einen E-Mail-Server ist der letzte von fünf Arbeitsschritten, die der Administrator ausführt, um beim Konfigurationsszenario für die LDAP-Authentifizierung und -Autorisierung den Zugriff auf die internen Netzwerkressourcen zu konfigurieren.

In diesem Beispiel sind im Netzwerk 10.10.0.0/24 drei E-Mail-Server installiert, wobei der Administrator den Remotebenutzern aus den Bereichen Vertrieb und Technik allerdings nur Zugriff auf einen dieser E-Mail-Server gewähren möchte. Der E-Mail-Server, auf den Remotebenutzer zugreifen müssen, hat die IP-Adresse 10.10.25.50/32.

Damit die Benutzer nur auf einen E-Mail-Server zugreifen können, erstellt der Administrator eine Anwendungsrichtlinie auf dem Access Gateway, nach der die Benutzer nur auf die E-Mail-Anwendung auf dem E-Mail-Server 10.10.25.50/32 zugreifen können.

Hinweis: Mit Anwendungsrichtlinien legen Administratoren fest, dass eine Clientanwendung auf einen bestimmten internen Server zugreifen oder ein Clientgerät bestimmte Anforderungen erfüllen muss, bevor der Zugriff auf einen internen Server zulässig ist.

Um eine Anwendungsrichtlinie zu erstellen, wonach der Zugriff eines E-Mail-Clients auf einen Server eingeschränkt wird, muss der Administrator drei Schritte ausführen:

- Erstellen einer Netzwerkressource, die nur den E-Mail-Server umfasst
- Erstellen einer Anwendungsrichtlinie, mit der die E-Mail-Anwendung auf dem E-Mail-Server angegeben wird, und Zuweisen der Netzwerkressource mit dem E-Mail-Server zu dieser Anwendungsrichtlinie
- Zuweisen der Anwendungsrichtlinie zu den Benutzergruppen im Access Gateway

In diesem Beispiel erstellt der Administrator eine Netzwerkressource namens „E-Mail-Server“, die nur die IP-Adresse 10.10.25.50/32 (den E-Mail-Server) enthält. Dann erstellt der Administrator eine Anwendungsrichtlinie namens „E-Mail-Anwendungsrichtlinie“, in der die E-Mail-Anwendung angegeben ist, auf die Remotebenutzer zugreifen können. Der Administrator weist dieser Anwendungsrichtlinie die Netzwerkressource „E-Mail-Server“ zu.

Danach fügt der Administrator den Gruppen „Vertriebsaußendienst“ und „Außendiensttechniker“ die „E-Mail-Anwendungsrichtlinie“ zu. Durch das Hinzufügen der Richtlinie zu diesen Gruppen ist gewährleistet, dass diese Gruppen stets auf die E-Mail-Anwendung auf dem vom Administrator in der Anwendungsrichtlinie angegebenen E-Mail-Server zugreifen.

So implementieren Sie die Anwendungsrichtlinie für den E-Mail-Server:

1. Erstellen Sie im rechten Bereich auf der Registerkarte **Access Policy Manager** im Access Gateway Administration Tool eine neue Netzwerkressource namens „E-Mail-Server“. Geben Sie für diese Netzwerkressource nur die IP-Adresse des E-Mail-Servers an, auf den die Benutzer zugreifen dürfen (z. B. 10.10.25.50/32). Diese Vorgehensweise ist im Wesentlichen identisch mit den vorigen Arbeitsschritten, bei denen die Netzwerkressourcen für die Benutzer in den Bereichen Vertrieb und Technik definiert wurden.
2. Klicken Sie mit der rechten Maustaste im rechten Bereich auf **Application Policies** und klicken Sie dann auf **New Application Policy**.
3. Geben Sie im Feld **Application Resource Name** „E-Mail-Anwendungsrichtlinie“ ein und klicken Sie auf **OK**.
4. Suchen und markieren Sie die E-Mail-Anwendung, die sich auf dem Server mit der IP-Adresse 10.10.25.50/32 befindet.

   Im Feld **MD5** wird automatisch die Binärsumme der Anwendung eingetragen.

5. Klicken Sie im linken Bereich auf die soeben erstellte Netzwerkressource „E-Mail-Server“ und ziehen Sie diese auf **Application network policies** unter dem Eintrag **Application Policies** im rechten Bereich. Klicken Sie auf **OK**.
6. Erweitern Sie im linken Bereich die Benutzergruppen „Vertriebsaußendienst“ und „Außendiensttechniker“.
7. Klicken Sie im rechten Bereich unter **Application Policies** auf die „E-Mail-Anwendungsrichtlinie“ und ziehen Sie diese auf **Application Policies** unter der Benutzergruppe „Vertriebsaußendienst“ im linken Bereich, sodass die Anwendungsrichtlinie ein Bestandteil der Zugriffssteuerungsliste für Außendienstmitarbeiter im Vertrieb ist.
8. Klicken Sie im rechten Bereich unter **Application Policies** auf die „E-Mail-Anwendungsrichtlinie“ und ziehen Sie diese auf **Application Policies** unter der Benutzergruppe „Außendiensttechniker“ im linken Bereich, sodass die Anwendungsrichtlinie ein Bestandteil der Zugriffssteuerungsliste für Außendiensttechniker ist.

Hinweis: Bei der oben beschriebenen Vorgehensweise könnte der Administrator der Anwendungsrichtlinie auch eine anwendungsspezifische Endpunktrichtlinie hinzufügen, wonach jedes Clientgerät beim Zugriff auf den E-Mail-Server bestimmte Anforderungen erfüllen muss. Weitere Informationen hierzu finden Sie unter „Festlegen von Anwendungsrichtlinien“ auf Seite 129.

Mit diesen Arbeitsschritten ist das Szenario für die Konfiguration der LDAP-Authentifizierung und -Autorisierung abgeschlossen. Danach hat der Administrator Folgendes konfiguriert:

- Benutzer können sich über ihre LDAP-Anmeldeinformationen bei dem LDAP-Verzeichnis authentifizieren, das im Authentifizierungsbereich **Default** angegeben ist.
- Auf Basis ihrer Gruppenmitgliedschaft im LDAP-Verzeichnis und auf dem Access Gateway dürfen Benutzer auf die internen Netzwerkressourcen zugreifen.

  Nur Benutzer, die Mitglied der Gruppe „Vertriebsaußendienst“ oder „Außendiensttechniker“ sind, dürfen auf Ressourcen im internen Netzwerk zugreifen. (Beide Gruppen müssen jeweils im LDAP-Verzeichnis und auf dem Access Gateway vorhanden sein.)
- Benutzer der Gruppe „Vertriebsaußendienst“ dürfen auf den Webkonferenzserver und die Dateiserver im Netzwerk 10.10.0.0/24 sowie auf die Webanwendung für den Vertrieb im Netzwerk 10.60.10.0/24 zugreifen.

Die Benutzer aus dem Bereich Vertrieb können zwar auf die E-Mail-Anwendung auf dem Server mit der IP-Adresse 10.10.25.50, jedoch nicht auf die E-Mail-Anwendung auf anderen E-Mail-Servern in den zugelassenen Netzwerken zugreifen.

Die Benutzer aus dem Bereich Vertrieb können auch auf andere Netzwerkressourcen zugreifen, die sich in den beiden zugelassenen Netzwerken befinden.

- Benutzer der Gruppe „Außendiensttechniker“ dürfen auf den Webkonferenzserver und die Dateiserver im Netzwerk 10.10.0.0/24 (und auf andere in diesem Netzwerk befindliche Netzwerkressourcen) zugreifen.

  Die Benutzer aus dem Bereich Technik können zwar auch auf die E-Mail-Anwendung auf dem Server mit der IP-Adresse 10.10.25.50, jedoch nicht auf die E-Mail-Anwendung auf anderen E-Mail-Servern in den zugelassenen Netzwerken zugreifen.

Nähere Informationen darüber, worin der Zweck von lokalen Benutzern auf dem Access Gateway besteht und wie die Authentifizierung und Autorisierung für lokale Benutzer zu ermöglichen ist, finden Sie unter„Szenario für das Erstellen von Gastkonten mit der Liste „Local Users““ auf Seite 325.

Szenario für das Erstellen von Gastkonten mit der Liste „Local Users“

Dieses Beispiel veranschaulicht die Funktionsweise von lokalen Benutzern auf dem Access Gateway und erläutert eine Methode, mit der ein Administrator die Authentifizierung und Autorisierung für lokale Benutzer unterstützen kann.

In dem zuvor beschriebenen Beispiel wurden Benutzer anhand ihrer Anmeldeinformationen für das LDAP-Verzeichnis und ihrer Gruppenmitgliedschaft authentifiziert und autorisiert.

Administratoren können auch eine Liste mit lokalen Benutzern auf dem Access Gateway erstellen und das Access Gateway so konfigurieren, dass diesen Benutzern Authentifizierungs- und Autorisierungsdienste zur Verfügung stehen. Diese Liste lokaler Benutzer wird in einer Datenbank auf dem Access Gateway, also nicht in einem externen Verzeichnis, verwaltet.

Lokale Benutzer eignen sich insbesondere, wenn der Administrator einen der folgenden Schritte ausführen möchte:

- Gewähren von Zugriff für Benutzer, die in keinem unternehmensinternen Verzeichnis aufgeführt sind
- Gewähren von Zugriff für Benutzer, die in einem unternehmensinternen Verzeichnis aufgeführt sind, zu dem das Access Gateway keine Verbindung herstellt
- Gewähren bestimmter Zugriffsrechte auf die internen Netzwerkressourcen für einen kleinen Benutzerkreis, ohne für diese Benutzer eine neue Gruppe im unternehmensinternen Verzeichnis erstellen zu müssen

Bei diesem Beispiel wird von Folgendem ausgegangen:

- Silvio Branco und Lisa Marth sind Berater, die nicht für das Unternehmen arbeiten und auch nicht im Unternehmensverzeichnis aufgeführt sind.
- Silvio Branco und Lisa Marth müssen Remotezugriff auf den Webkonferenzserver im internen Netzwerk haben, damit sie an Konferenzen mit Benutzern aus den Bereichen Vertrieb und Technik teilnehmen können, die Angestellte des Unternehmens sind.
- Der Administrator hat die weiter oben in diesem Kapitel beschriebene LDAP-Authentifizierung und -Autorisierung bereits konfiguriert, sodass Benutzer aus den Bereichen Vertrieb und Technik auf den Webkonferenzserver zugreifen können.
- Der Webkonferenzserver hat die IP-Adresse 10.10.50.60.

Hinweis: In diesem Beispiel werden Silvio Branco und Lisa Marth als Gastbenutzer angesehen, weil sie keine Angestellten des Unternehmens und auch nicht im Unternehmensverzeichnis aufgeführt sind.

Um Silvio Branco und Lisa Marth Zugriff auf den Webkonferenzserver zu gewähren, führt der Administrator die folgenden drei Schritte aus:

- Erstellen eines Authentifizierungsbereichs für Gastbenutzer
- Erstellen von lokalen Benutzern
- Erstellen und Zuweisen einer Netzwerkressource für die Standardbenutzergruppe **Default** auf dem Access Gateway

Erstellen eines Authentifizierungsbereichs für Gastbenutzer

Das Erstellen eines Authentifizierungsbereichs für Gastbenutzer ist der erste von drei Arbeitsschritten, die der Administrator beim Szenario für das Erstellen von Gastkonten mit der Liste **Local Users** ausführt.

Beim vorigen Szenario für die Konfiguration von LDAP-Authentifizierung und -Autorisierung hat der Administrator einen Standardauthentifizierungsbereich (**Default**) erstellt, um die Authentifizierung und Autorisierung der in einem unternehmensinternen LDAP-Verzeichnis aufgeführten Benutzer zu unterstützen.

Da Silvio Branco und Lisa Marth nicht im unternehmensinternen LDAP-Verzeichnis aufgeführt sind, erstellt der Administrator einen separaten Authentifizierungsbereich für sie, der Folgendes unterstützt:

- **Lokale Authentifizierung:** Diese Option in einem Authentifizierungsbereich gewährleistet, dass Benutzer anhand einer Liste **Local Users** auf dem Access Gateway und nicht auf Basis eines externen Verzeichnisses authentifiziert werden.
- **Keine Autorisierung:** Diese Option in einem Authentifizierungsbereich gewährleistet, dass Benutzern dieses Bereichs die mit der Benutzergruppe **Default** auf dem Access Gateway verknüpften Zugriffsrechte gewährt werden.

So erstellen Sie einen Authentifizierungsbereich für die Gastbenutzer:

1. Klicken Sie im Access Gateway Administration Tool auf die Registerkarte **Authentication**.
2. Geben Sie im Feld **Realm name** den Namen **Gast** ein.
3. Wählen Sie **One Source** und klicken Sie auf **Add**.
4. Aktivieren Sie im Dialogfeld **Select Authentication Type** die Option **Local authentication only** und klicken Sie dann auf **OK**.
5. Aktivieren Sie auf der Registerkarte **Authorization** die Option **No authorization**.
6. Klicken Sie auf **Submit**.

Erstellen lokaler Benutzer

Das Erstellen von lokalen Benutzern ist der zweite von drei Arbeitsschritten, die der Administrator beim Szenario für das Erstellen von Gastkonten mit der Liste **Local Users** ausführt.

Bei diesem Arbeitsschritt erstellt der Administrator lokale Benutzerkonten für Silvio Branco und Lisa Marth auf dem Access Gateway und gibt beiden Benutzern jeweils ein Kennwort.

So fügen Sie lokale Benutzer hinzu:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Klicken Sie mit der rechten Maustaste auf **Local Users** und wählen Sie dann die Option **New User**.
3. Geben Sie im Feld **User Name** Lisa Marth ein.
4. Geben Sie in den Feldern **Password** und **Verify Password** ein Kennwort für Lisa Marth ein und klicken Sie auf **OK**.
5. Wiederholen Sie die Schritte 2 bis 4, um ein lokales Benutzerkonto für Silvio Branco zu erstellen.

Erstellen und Zuweisen einer Netzwerkressource für die Standardbenutzergruppe

Das Erstellen und Zuweisen einer Netzwerkressource für die Standardbenutzergruppe **Default** ist der letzte von drei Arbeitsschritten beim Szenario für das Erstellen von Benutzerkonten mit der Liste **Local Users**.

Bei diesem Schritt erstellt der Administrator eine Netzwerkressource, in der nur der Webkonferenzserver angegeben ist, und weist dann diese Ressource der Benutzergruppe **Default** zu.

1. Erstellen Sie im rechten Bereich der Registerkarte **Access Policy Manager** im Administration Tool eine neue Netzwerkressource namens „Gastressource“. Geben Sie beim Erstellen dieser Netzwerkressource nur die IP-Adresse des Webkonferenzservers an (z. B. 10.10.50.60/32).
2. Erweitern Sie im linken Bereich die Benutzergruppe **Default**.

3. Ziehen Sie die Netzwerkressource „Gastressource“ aus dem rechten Bereich der Registerkarte **Access Policy Manager** auf **Network Policies** der Gruppe **Default** im linken Bereich.

Hinweis: Wenn sich ein Benutzer anmeldet und keine Gruppeninformationen abrufen kann, verwendet er stets die Einstellungen der Gruppe **Default**.

Nach Ausführung dieser Arbeitsschritte hat der Administrator Folgendes bewirkt:

- Silvio Branco und Lisa Marth können die Benutzeranmeldeinformationen „Gast\Silvio Branco“ oder „Gast\Lisa Marth“ zur Authentifizierung beim Bereich **Gast** auf dem Access Gateway eingeben. Bei der Authentifizierung müssen Silvio Branco und Lisa Marth den Bereichsnamen als Bestandteil ihrer Benutzeranmeldeinformationen einschließen, da sie sich bei einem Bereich authentifizieren, der nicht der Authentifizierungsbereich **Default** ist.

  Silvio Branco und Lisa Marth verwenden außerdem das Kennwort, das der Administrator für sie für die Authentifizierung beim Access Gateway festgelegt hat. Der Administrator hat diese Kennwörter beim Erstellen von Silvio Branco und Lisa Marth als lokale Benutzer auf dem Access Gateway eingegeben.

- Silvio Branco und Lisa Marth dürfen auf alle in der Zugriffssteuerungsliste der Benutzergruppe **Default** definierten Ressourcen zugreifen, da **No authorization** als Autorisierungstyp des Bereichs **Guest** angegeben ist.

  In diesem Beispiel können Silvio Branco und Lisa Marth nur auf den Webkonferenzserver im internen Netzwerk zugreifen, weil nur diese Netzwerkressource für die Benutzergruppe **Default** definiert ist.

Szenario für das Konfigurieren der lokalen Autorisierung für lokale Benutzer

Durch geringfügiges Ändern der unter „Szenario für das Erstellen von Gastkonten mit der Liste „Local Users““ beschriebenen Konfiguration kann der Administrator lokalen Benutzern (Lisa Marth und Silvio Branco) die gleichen Zugriffsrechte auf die internen Netzwerkressourcen gewähren wie den Benutzern aus den Bereichen Vertrieb oder Technik.

In diesem Szenario wird das Konzept der lokalen Autorisierung für lokale Benutzer erläutert.

Beispiel: Der Administrator möchte Lisa Marth und Silvio Branco die gleichen Zugriffsrechte gewähren wie den Benutzern aus dem Bereich Technik. Zu diesem Zweck könnte der Administrator zwei Arbeitsschritte ausführen:

- Ändern des Autorisierungstyps des Bereichs **Gast** in lokale Autorisierung
- Zuweisen der lokalen Benutzer Lisa Marth und Silvio Branco zur Gruppe „Außendiensttechniker“ auf dem Access Gateway

Um die lokalen Benutzer Lisa Marth und Silvio Branco der Gruppe „Außendiensttechniker“ auf dem Access Gateway zuzuweisen, geht der Administrator wie folgt vor:

1. Klicken Sie auf die Registerkarte **Access Policy Manager**.
2. Erweitern Sie den Eintrag **User Groups** und dann den Eintrag **Local Users**.
3. Klicken Sie unter **Local Users** auf den Namen Lisa Marth und ziehen Sie ihren Namen auf **Local Group Users** unter der Benutzergruppe „Außendiensttechniker“.
4. Klicken Sie unter **Local Users** auf den Namen Silvio Branco und ziehen Sie seinen Namen auf **Local Group Users** unter der Benutzergruppe „Außendiensttechniker“.

Nach Ausführung dieses Arbeitsschritts treffen die beiden folgenden Aussagen zu:

- Silvio Branco und Lisa Marth können die Benutzeranmeldeinformationen „Gast\Silvio Branco“ oder „Gast\Lisa Marth“ zur Authentifizierung beim Bereich **Gast** auf dem Access Gateway eingeben.
- Silvio Branco und Lisa Marth dürfen auf alle in der Zugriffssteuerungsliste der Benutzergruppe „Außendiensttechniker“ definierten Ressourcen zugreifen, da **Local authorization** als Autorisierungstyp für den Bereich **Gast** angegeben ist.

  Hierdurch erhalten lokale Benutzer dieselbe Autorisierung wie die Benutzergruppe auf dem Access Gateway, der sie zugewiesen sind. Ihnen wird nicht die mit der Benutzergruppe **Default** auf dem Access Gateway verknüpfte Autorisierung erteilt, wie es der Fall ist, wenn **No authorization** für den Authentifizierungsbereich **Gast** aktiviert ist.

Problembehandlung beim Access Gateway

Im Folgenden wird erläutert, was Sie bei Problemen tun können, die beim Einrichten und Verwenden des Access Gateways auftreten.

Problembehandlung bei Webinterface-Verbindungen

In diesem Abschnitt werden Probleme erläutert, die beim Herstellen einer Verbindung zum Webinterface auftreten können.

Das Webinterface wird angezeigt, ohne dass Anmeldeinformationen eingegeben wurden

Wenn Sie die Webadresse für das Access Gateway eingegeben haben, wird das Webinterface angezeigt, ohne dass der Benutzername und das Kennwort eingegeben werden mussten. Die Ursache für dieses Verhalten besteht darin, dass Sie die Portalseitenauthentifizierung deaktiviert haben. Aktivieren Sie im Administration Tool auf der Registerkarte **Global Cluster Policies** unter **Advanced options** die Option **Enable logon page authentication**.

Wenn diese Option deaktiviert ist, wird nicht authentifizierter Netzwerkverkehr an das Webinterface gesendet. Dies ist zwar eine gültige Konfiguration, Sie müssen aber sicherstellen, dass sich das Webinterface in der DMZ befindet.

Nach dem Anmelden werden keine Anwendungen angezeigt

Benutzer, die sich am Access Gateway anmelden, bekommen ihre Anwendungen nicht angezeigt. Das Message Center gibt an, dass keine Domäne festgelegt wurde.

Standardmäßig übergibt das Access Gateway nur den Benutzernamen und das Kennwort an das Webinterface. Um dieses Problem zu beheben, konfigurieren Sie in der Access Management Console eine Standarddomäne oder eine Domänenliste, an denen sich der Benutzer anmelden kann. Das Webinterface verwendet die in der Liste an erster Stelle stehende Domäne als Standarddomäne.

Benutzer, die sich am Access Gateway anmelden, bekommen zwar das Webinterface, nicht aber ihre Anwendungen angezeigt. Das Message Center gibt an, dass die Anmeldeinformationen des Benutzers ungültig sind.

Die wahrscheinlichste Ursache für diese Fehlermeldung besteht darin, dass die Benutzer sich am Access Gateway mit Nicht-LDAP-Anmeldeinformationen von einer anderen Domäne als der Domäne anmelden, für die das Webinterface eingerichtet ist. Zur Lösung dieses Problems müssen Sie sicherstellen, dass die Standarddomäne auf dem Server, auf dem das Webinterface ausgeführt wird, mit dem Standardbereich im Access Gateway identisch ist. Stellen Sie außerdem sicher, dass das Access Gateway für LDAP-Authentifizierung konfiguriert ist und dass der LDAP-Server ein Domänencontroller in derselben Domäne wie das Webinterface ist.

Benutzer könnten sich auch mit einem Bereichsnamen am Access Gateway anmelden, aber der Bereichsname ist nicht derselbe wie der Domänenname. Bereichsnamen müssen mit den entsprechenden Active Directory-Domänennamen übereinstimmen. Damit sich Benutzer mit einem anderen Bereichsnamen als dem des Standardbereichs anmelden können, geben Sie den Bereichsnamen und den Benutzernamen ein, z. B. *Bereichsname\Benutzername*. Wenn sich die Benutzer am Access Gateway anmelden, werden dann der Bereichsname und der Benutzername an das Webinterface übergeben. Das Webinterface wandelt den Bereichsnamen und den Benutzernamen in den Domänennamen und Benutzernamen um.

Benutzer werden zu einer Anmeldeseite geleitet, auf der sie zum Starten des Secure Access Clients aufgefordert werden

In den Gruppeneigenschaften der Standardgruppe, bzw. der Gruppe mit der höchsten Priorität, des Benutzers ist auf der Registerkarte **Gateway Portal** die Option **Use the multiple logon option page** aktiviert. Wenn Sie dem Benutzer keinen Zugriff auf den Secure Access Client geben möchten, deaktivieren Sie dieses Kontrollkästchen. Weitere Informationen hierzu finden Sie unter „Konfigurieren einer Portalseite mit mehreren Anmeldeoptionen“ auf Seite 190.

So deaktivieren Sie die Seite mit mehreren Anmeldeoptionen:

1. Klicken Sie mit der rechten Maustaste auf der Registerkarte **Access Policy Manager** auf eine Gruppe und klicken Sie dann auf **Properties**.
2. Deaktivieren Sie auf der Registerkarte **Gateway Portal** die Option **Use the multiple logon option page**.
3. Klicken Sie auf **OK**.

Sonstige Probleme

In diesem Abschnitt werden bekannte Probleme, die im Zusammenhang mit dem Access Gateway auftreten, sowie entsprechende Lösungsvorschläge beschrieben.

Lizenzdatei stimmt nicht mit dem Access Gateway überein

Wenn Sie versuchen, eine Lizenzdatei auf dem Access Gateway zu installieren, wird die Fehlermeldung „License file does not match any Access Gateway's" angezeigt. Auf dem Access Gateway ist dann bereits eine Lizenzdatei installiert. Wenn Sie eine neue Lizenzdatei hochladen möchten, muss die alte Lizenz entfernt werden.

So installieren Sie eine neue Lizenzdatei auf dem Access Gateway:

1. Wählen Sie auf der Registerkarte **Access Gateway Cluster** das Access Gateway aus, dem Sie die Lizenz hinzufügen möchten.
2. Klicken Sie auf der Registerkarte **Licensing** neben **Remove all license files** auf **Remove All**.
3. Starten Sie das Access Gateway neu.
4. Klicken Sie auf der Registerkarte **Licensing** neben **Install a license file** auf **Browse** und navigieren Sie zur Lizenzdatei.
5. Klicken Sie auf **Öffnen**, um die Datei zu installieren.
6. Starten Sie das Access Gateway neu.

Definieren von Subnetzeinschränkungen für zugängliche Netzwerke

Im Feld **Accessible Networks** auf der Registerkarte **Global Cluster Policies** können bis zu 24 Subnetze definiert werden. Wenn mehr als 24 Subnetze angegeben werden, ignoriert das Access Gateway die überzähligen Einträge.

VMWare

Wenn ein Benutzer sich auf dem Secure Access Client von zwei Computern aus anmeldet, auf denen VMWare ausgeführt wird, und VMWare für beide Computer dieselbe MAC-Adresse verwendet, lässt das Access Gateway nicht zu, dass beide Clients gleichzeitig ausgeführt werden. Das Access Gateway verwendet die MAC- Adresse zum Verwalten der Lizenzen und lässt immer nur eine Clientsitzung pro MAC-Adresse gleichzeitig zu.

ICMP-Übertragungen

Wenn eine ICMP-Übertragung aus irgendeinem Grund fehlschlägt, gibt das Access Gateway eine „Request timed out“-Fehlermeldung zurück. Wenn ein Client versucht, das Access Gateway zu pingen, sendet es immer ein ICMP-Standardpaket an den Remotezielhost. Sämtliche Clientoptionen, wie z. B. das Erhöhen der Größe der ICMP-Nutzlast, werden vom Access Gateway nicht anerkannt und auch nicht an den Remotehost gesendet.

Ping-Befehl

Das Access Gateway sendet grundsätzlich denselben ping-Befehl aus, und dies unabhängig von den Optionen, die beim Pingen von einem Clientgerät aus angegeben werden.

LDAP-Authentifizierung

Wenn das Access Gateway für die Verwendung der LDAP-Authentifizierung und -Autorisierung konfiguriert ist, werden die LDAP-Gruppeninformationen nicht zum automatischen Ausfüllen des Gruppenfelds im Administration Tool verwendet.

Endpunktrichtlinien

Bei der Auswertung der Kombination von Endpunktrichtlinien einer Gruppe berücksichtigt das Access Gateway nicht die Gruppenprioritäten, sodass miteinander in Konflikt stehende Richtlinien u. U. nicht korrekt aufgelöst werden. Nur die Richtlinie, die im Ausdruck zuletzt aufgeführt wird, gilt. Wenn z. B. für eine Gruppe die Richtlinie „ProzessA“ und für eine andere Gruppe die Richtlinie „!ProzessA“ gilt und die Kombination aus diesen beiden Richtlinien „ProzessA and !ProzessA“ lautet, gilt nur die Richtlinie „!ProzessA“.

Netzwerkressourcen

Bei hinzugefügten Netzwerkressourcen erkennt das Access Gateway nicht die CIDR-Notation der Adresse *IP-Adresse*/0. Wenn Sie z. B. eine Ressourcengruppe hinzufügen möchten, die den Zugriff auf alle Ressourcen erlaubt, geben Sie die Adresse in der Form „0.0.0.0/0.0.0.0“ statt in der Form „0.0.0.0/0“ an.

Kioskverbindungen

Für Kioskverbindungen muss das Access Gateway ein Zertifikat besitzen, das von einer für Sun Microsystems vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Für Clientverbindungen im Kioskmodus muss JRE (Java Runtime Environment) 1.5 auf den Computern installiert sein.

Internes Failover

Wenn das interne Failover aktiviert ist und der Administrator eine Verbindung zum Access Gateway hergestellt hat, ist das Administration Tool über diese Verbindung nicht erreichbar. Aktivieren Sie zum Beseitigen dieses Problems das IP-Pooling und stellen Sie dann eine Verbindung zur niedrigsten IP-Adresse im IP-Pool auf Port 9001 her. Wenn der IP-Pool z. B. bei 10.10.3.50 beginnt, stellen Sie die Verbindung zum Administration Tool unter Verwendung von 10.10.3.50:9001 her. Informationen zum Konfigurieren von IP-Pools finden Sie unter „Aktivieren von IP-Pooling“ auf Seite 168.

Zertifikatsignierung

Zahlreiche Citrix Serverkomponenten unterstützen SSL/TLS, z. B. Access Gateway, Secure Gateway und SSL Relay. Alle diese Komponenten unterstützen Serverzertifikate, die von einer öffentlichen oder einer privaten Zertifizierungsstelle (CA, Certificate Authority) ausgegeben wurden. Beispiele für öffentliche Zertifizierungsstellen sind Organisationen wie Verisign und Thawte. Private Zertifizierungsstellen werden durch Produkte, wie z. B. Microsoft Zertifikatdienste, implementiert.

Zertifikate, die von einer privaten Zertifizierungsstelle signiert wurden, werden mitunter als *Unternehmenszertifikate* oder *selbst signierte Zertifikate* bezeichnet. Der Begriff „selbst signiertes Zertifikat“ ist in diesem Zusammenhang technisch unkorrekt, da die Zertifikate von der privaten Zertifizierungsstelle signiert werden. Wirklich selbst signierte Zertifikate werden hingegen nicht von einer Zertifizierungsstelle signiert und auch nicht von Citrix Serverkomponenten unterstützt, da dann keine vertrauenswürdige Zertifizierungsstelle dahinter steht. Wie bereits oben erwähnt, werden aber von einer privaten Zertifizierungsstelle ausgegebene Zertifikate von Citrix Serverkomponenten unterstützt, da der privaten Zertifizierungsstelle vertraut werden kann.

Zertifikatsperrlisten

Zertifikatsperrlisten (Certificate Revocation Lists, CRLs) können nicht vom Administrator konfiguriert werden. Wenn ein Benutzer eine Verbindung zum Access Gateway unter Verwendung eines Clientzertifikats herstellt, verwendet das Access Gateway die CRLDistributionPoints-Erweiterung im Clientzertifikat, sofern vorhanden, um über HTTP nach relevanten CRLs zu suchen. Das Clientzertifikat wird dann mit diesen CRLs abgeglichen.

Netzwerkmeldungen an nicht vorhandene IP-Adressen

Wenn die auf das Access Gateway hochgeladene Datei sdconf.rec ungültig ist, sendet das Access Gateway u. U. Meldungen an nicht vorhandene IP-Adressen. Netzwerküberwachungseinrichtungen könnten dies als Netzwerkspamming einstufen.

Dieses Problem können Sie beseitigen, indem Sie eine gültige sdconf.rec-Datei auf das Access Gateway hochladen.

Das Access Gateway startet nicht und die serielle Konsole ist leer

Überprüfen Sie die folgenden Elemente auf ihre korrekte Einrichtung:

- Die serielle Konsole verwendet den richtigen Port und der physische Port stimmt mit dem logischen Port überein.
- Das Kabel ist ein Nullmodemkabel.
- Die COM-Einstellungen der seriellen Kommunikationssoftware sind wie folgt festgelegt: 9600 Bit/s, 8 Datenbits, keine Parität und 1 Stoppbit.

Zugriff auf das Administration Tool nicht möglich

Wenn das Access Gateway offline ist, ist das Administration Tool nicht verfügbar. Zum Ausführen von Aufgaben wie dem Anzeigen des Systemprotokolls und dem Neustarten des Access Gateways können Sie das Administration Portal verwenden.

Kommunikation zwischen Geräten und dem Access Gateway nicht möglich

Überprüfen Sie die folgenden Elemente auf ihre korrekte Einrichtung:

- Der auf der Registerkarte **General Networking** im Access Gateway Administration Tool angegebene vollqualifizierte Domänenname ist außerhalb Ihrer Firewall verfügbar.
- Sämtliche Änderungen, die in der seriellen Konsole des Access Gateways oder im Administration Tool vorgenommen wurden, wurden gesendet.

Verwenden von Strg+Alt+Entf zum Neustarten des Access Gateways nicht möglich

Die Neustartfunktion auf dem Access Gateway ist deaktiviert. Sie müssen das Gerät mit dem Administration Tool neu starten und herunterfahren.

Sitzungen mit SSL Version 2 und Zertifikatketten auf mehreren Ebenen

Wenn Zwischenzertifikate (Zertifikate mit mehreren Ebenen) Teil Ihres sicheren Zertifikatsuploads sind, stellen Sie sicher, dass die Zwischenzertifikate in der hochzuladenden Zertifikatdatei enthalten sind. SSL Version 2 unterstützt die Zertifikatsverkettung nicht. Alle Zertifikate, die mehr als eine Ebene besitzen, müssen sämtliche Zwischenzertifikate enthalten, da das System anderenfalls unbrauchbar werden könnte. Informationen dazu, wie Sie der hochzuladenden Zertifikatdatei Zwischenzertifikate hinzufügen können, finden Sie unter „Sichern von Verbindungen mit digitalen Zertifikaten“ auf Seite 291.

H.323-Protokoll

Das Access Gateway unterstützt das H.323-Protokoll nicht. Anwendungen, die das H.323-Protokoll verwenden, wie z. B. NetMeeting von Microsoft, können mit dem Access Gateway nicht verwendet werden.

Zertifikate mit 512-Bit-Schlüsselpaaren

Verwenden Sie zum Konfigurieren von Zertifikaten keine 512-Bit-Schlüsselpaare, da diese oft Opfer von Brute-Force-Angriffen werden.

Laufwerkszuordnung kann nicht mit einer Anwendungsrichtlinie eingeschränkt werden

Sie können nicht mit einer Anwendungsrichtlinie Benutzeraktivitäten, die direkt innerhalb des Windows-Betriebssystems verarbeitet werden, z. B. die Laufwerkszuordnung, einschränken. Hierfür müssen Sie eine Netzwerkgruppenrichtlinie verwenden.

Beispiel: Wenn Sie verhindern möchten, dass Benutzer in der Standardbenutzergruppe in Windows-Explorer eine Verknüpfung mit Laufwerken im Subnetz 10.51.251.0/24 herstellen, müssen Sie eine Gruppenressource erstellen, in der dieses Subnetz angegeben wird, und diese Ressource der Standardgruppe zuweisen. Verweigern Sie dann den Zugriff auf diese Netzwerkressource.

Sie können den Zugriff nicht durch Erstellen einer Anwendungsrichtlinie für Windows-Explorer einschränken, in die eine Netzwerkressource eingebettet ist, auf die der Zugriff Netzwerkressource verweigert ist.

Secure Access Client

Im Zusammenhang mit dem Secure Access Client können die im Folgenden beschriebenen Probleme auftreten.

Secure Access Client-Verbindungen mit Windows XP

Wenn ein Windows XP-Benutzer eine Verbindung zum Access Gateway herstellt, den Computer abmeldet, ohne vorher die Verbindung zum Secure Access Client zu trennen, und sich dann wieder anmeldet, ist die Internetverbindung unterbrochen. Zum Wiederherstellen der Internetverbindung müssen Sie den Computer neu starten.

DNS-Namensauflösung mit Namensdienstanbietern

Wenn Clients ohne administrative Berechtigungen über Windows 2000 Professional oder Windows XP eine Verbindung zum Access Gateway herstellen, kann die DNS-Namensauflösung scheitern, wenn der Client einen Namensdienstanbieter verwendet. Dieses Problem lässt sich beheben, indem die Verbindung nicht mit dem DNS-Namen, sondern mit der IP-Adresse des Computers hergestellt wird.

Funktion zum automatischen Aktualisieren

Die Secure Access Client-Funktion zum automatischen Aktualisieren funktioniert nicht, wenn der Client für das Herstellen der Verbindung über einen Proxyserver konfiguriert ist.

Von Windows Server 2003-Computern ausgehende Clientverbindungen

Wenn von einem Windows Server 2003-Computer aus eine Verbindung zum Access Gateway hergestellt wird, der sein eigener DNS-Server ist, funktionieren die lokale und die öffentliche DNS-Auflösung nicht. Dieses Problem können Sie beheben, indem die Windows Server 2003-Netzwerkeinstellungen auf einen anderen DNS-Server verweisen.

NTLM-Authentifizierung

Der Secure Access Client bietet keine Unterstützung für die NTLM-Authentifizierung gegenüber von Proxyservern. Bei Proxyservern wird lediglich die einfache Authentifizierung unterstützt.

WINS-Einträge

Wenn die Verbindung zum Secure Access Client getrennt wird, werden WINS-Einträge nicht von dem Computer entfernt, auf dem der Client ausgeführt wird.

Benutzer von Einwählverbindungen erhalten keine WINS-Serverzuordnungen. Legen Sie zur Behebung dieses Problems die interne WINS-Adresse manuell fest oder verwenden Sie einen DNS-Server von Microsoft zum Festlegen der Domäne für die WINS-Suche.

Verwendung von Drittanbieter-Clientsoftware

Wenn auf dem Computer eines Benutzers der Secure Access Client ausgeführt wird, auf diesem Computer aber auch VPN-Software eines Drittanbieters installiert ist und die Verbindungen nicht korrekt über das Access Gateway ausgeführt werden, vergewissern Sie sich, dass die Drittanbieteranwendung deaktiviert oder ausgeschaltet ist. Testen Sie anschließend die Secure Access Client-Verbindung erneut.

Index

A

Access Gateway
  Aktualisieren 261
  Betriebsmodi 18
  Herunterfahren 266
  In einer Double-Hop-DMZ installieren 235
  Mehrere Geräte lizenzieren 52
  Migrieren von Secure Gateway 201
  Neustart 48, 265
  Statistiken 288
  Überwachen 288
  Verbindungen 18
  Wartung 255
Access Gateway Advanced Edition 19, 37
  Clientzertifikate 178
  Inaktiver Server 38
ACL, *siehe* Zugriffssteuerungsliste
Active Directory
  Anmeldeskripte 22
ActiveX-Steuerelement
  Portalseite 188
  Secure Access Client 152
Administration Desktop
  Ethereal Network Analyzer 289
  fnetload 290
  Gruppenprioritäten 137
  Herunterladen oder Starten 258
  Öffnen 260, 289
  Real-time Monitor 289
  System Monitor 290
  Traceroute 289
  Überwachungstools 288
  xNetTools 289
Administration Portal
  Administratorkennwort 258
  Deaktivieren des externen Zugriffs mit dem Administration Tool 259
  Externen Zugriff mit der seriellen Konsole deaktivieren 43
  Port 25
  Protokollierung 259
  Verfügbare Downloads 258
  Wartung 259
  Webadresse 260
  Zertifikate installieren 59
Administration Tool
  Downloaden 258
  In einer Double-Hop-DMZ installieren 232
  Installation 45, 256
  Internes Failover 335
  Port 25
  Protokollierung 259
  Zugriff nicht möglich 336
Administratoren
  Secure Access Client 149
Administratorkennwort
  Administration Portal 258
  Serielle Konsole 43
AES 20
Aktualisieren 16
  Access Gateway-Software 261
  Secure Access Client 151
Anmeldeseite 120
  Aktivieren 183
  Authentifizierung 207
  Authentifizierung deaktivieren 190
  Authentifizierung in Double-Hop-DMZ 230
  Authentifizierung in Double-Hop-DMZ aktivieren 230
  Webinterface 216
Anmeldeskripte 22, 170
Anwendungen
  Kioskmodus 158

Anwendungsrichtlinien 120, 129
Einschränken der Laufwerkszuordnung nicht möglich 337
Konfigurationsbeispiel 322
Zulassen und Verweigern 127
Archiv des Systemprotokolls 283
Asymmetrische Verschlüsselung 293
Auslagerungsbereichsnutzung 290
Authentifizierung 97
Aktivieren der Anmeldeseite 183
Anmeldeseite 207
Anmeldeseite deaktivieren 190
Anmeldeseite in Double-Hop-DMZ 230
Anmeldeseite in Double-Hop-DMZ aktivieren 230
Benutzergruppe 118
Bereiche 82
Default (Bereich) 80
ICA-Zugriffssteuerung 214
Konfigurieren 78
LDAP 86, 142
LDAP-Konfigurationsbeispiel 309, 317
Lokal 83, 142
Lokale Benutzer 84
Mit zwei Methoden 110, 191
Netzwerkunterbrechung 167
NTLM 107, 142, 339
Ohne Autorisierung 80
RADIUS 95, 142
RSA SecurID 100, 142
RSA SecurID aktivieren 102
SafeWord 104, 142
Webinterface 193, 207
Zertifikate 295
Authentifizierungsarten 28
Autorisierung 80
LDAP 86, 90
LDAP-Konfigurationsbeispiel 309
Lokale Benutzer 84
NTLM 109
RADIUS 95, 98
SafeWord 106

B

Benutzer
Anzeigen von Gruppen und Prioritäten 137
Deaktivieren und Aktivieren 175
Mehreren Gruppen hinzufügen 124
Mit freigegebenen Netzlaufwerken arbeiten 166
Netzwerkzugriff 114
Offene Verbindungen anzeigen 289
Benutzergruppen
Authentifizierung 118
Benutzer 117
Desktopfreigaben deaktivieren 173
Eigenschaften 122, 168
Entfernen 122
Erstellen 121
Gruppenpriorität 137
IP-Pooling 168
Konfigurieren 117
Lokal 119
Mehrere 121
Portalseite 190
Ressourcen 123
Ressourcenzugriffssteuerung 128
Sitzungstimeout aktivieren 171
Split DNS 169
Übersicht 118
Benutzergruppeninformationen 118
Benutzerkennwörter 85
Benutzername (Variable für Portalseite) 186
Benutzersitzungstimeout 21, 171
Benutzerverbindungen
Citrix Presentation Server 194
Secure Access Client 139, 195
Bereiche
Entfernen 83
Erstellen 82
Bereichsbasierte Authentifizierung
Default (Bereich) 80
Bereitstellung
Access Gateway Advanced Edition 37
Citrix Presentation Server 28
Cluster 273
Double-Hop-DMZ 20, 33, 228
Einzelne DMZ 24
Failover 35, 280
Load Balancer 35, 275
Mehrere Access Gateway-Geräte 271
Sicheres Netzwerk 26
Überlegungen zur Sicherheit 27
Unterstützung bei der Authentifizierung 28
Webinterface 28, 30
Bereitstellungsoptionen 23
Beschriftung von Kennwortfeldern 111, 156
Betriebsmodi 18
BlackICE PC Protection 268

C

CIFS/SMB 165
Citrix Preferred Support Services 15
Citrix Presentation Server 18, 120
  Bereitstellung 28
  Double-Hop-DMZ-Bereitstellung 20, 223
  ICA-Zugriffssteuerung 214
  Konfigurieren des Netzwerkzugriffs 214
  Konfigurieren von Benutzerverbindungen 194
  Serverfarm 193
  Split-Tunneling 117
Citrix Presentation Server Clients 18, 195
  Gleichzeitige Verbindung mit Secure Access Client 195
Citrix Schulungen 16
Citrix Solutions Advisors 15
Clients
  Kioskmodus 19
  Stammzertifikate 179
Clientvariablen für Portalseite 186
Clientverbindungsprotokolle 285
Clientzertifikate 120, 176
  Access Gateway Advanced Edition 178
  Kriterien festlegen 177
Clientzugriff
  IP-Pooling 120
  Portalseite 190
  Ressourcenzugriffssteuerung 128
  Sitzungstimeout 119
  Split DNS 120
  Zertifikate 120
Cluster
  Erstellen 273
  RSA SecurID 103
Clusterbereitstellung 273
Computer
  Ruhezustand 167
  Standby-Modus 167
CPU-Auslastung 290
CRLs, *siehe* Zertifikatsperrlisten

D

Dateifreigabe
  Bereitstellungsart 165
  Ressourcen 166
Dateifreigaben
  Kioskmodus 158
  Konfigurieren 165
Dateifreigaberessourcen 120
Datenverschlüsselung 20
Datum
  Einstellungen 70
Deaktivieren der Desktopfeigabe 21
Default (Bereich) 80
Desktopfreigabe 21
  Deaktivieren 173
Dienstscanner 289
DNS
  Failover auf lokales DNS 62
  Namensauflösung 338
  Secure Access Client-Fenster 157
  Servereinstellungen 62
DNS/WINS
  siehe Namensdienstanbieter
Dokumentation 15
  Herunterladen 258
Domänenanmeldeskripte 170
Double-Hop-DMZ 20, 33, 223
  Access Gateway installieren 235
  Anmeldeseitenauthentifizierung 230
  Bereitstellung 228
  Installation des Administration Tools 232
  Komponenten 234
  Lastausgleich 229
  Ports 234, 245
  TCP/IP-Einstellungen 48
  Verbindungsprozess 225
  Zertifikate 234
Downloads
  Access Gateway-Dokumentation 258
  Administration Desktop 258
  Administration Tool 258
  Portalseitenvorlagen 258
  Vom Administration Portal 258
Duplex Mode 46
Dynamisches Routing 64, 66
  In statischer Routentabelle speichern 66
  RIP-Authentifizierung aktivieren 65

E

Eigenschaften
  Benutzergruppen 122
  Gruppe 119
  Secure Access Client 268
Eigenständige Bereitstellung 18
Eingabeaufforderung
  Mehrere Stammzertifikate erstellen 62
Endpunktressourcen
  Entfernen 133
  Konfigurieren 131

Endpunktrichtlinie
Ausdruck erstellen 134
Erstellen 134
Für Gruppe konfigurieren 133
Gültige Operatoren 134
Problembehandlung 334
Entfernen von Bereichen 83
Ersetzen von Secure Gateway 197
Ethereal Network Analyzer 289
Unverschlüsselter Datenverkehr 145
Express Setup
Serielle Konsole 43

F

Failover 35
Bereitstellung 280
DNS-Server 62
Intern 170
Konfigurieren 280
Federal Information Processing Standard 292
Fingerabfrage 289
FIPS 140, *siehe* Federal Information Processing Standard
Firefox 160
Kioskmodus 158
Firewall
BlackICE PC Protection 268
Lizenzierung 53
McAfee Personal Firewall Plus 268
Mit Secure Access Client verwenden 143
Norton Personal Firewall 269
Sygate Personal Firewall 269
Tiny Personal Firewall 269
ZoneAlarm Pro 270
fnetload-Tool 290
Freigegebene Netzlaufwerke 158, 166
FTP
Für die Verwendung mit Clients konfigurieren 147
In Kiosksitzung verwenden 166

G

Gaim 158, 164
Gemeinsamer geheimer Schlüssel 103
Gruppen
Benutzer hinzufügen 124
Gruppenattribute
LDAP-Autorisierung 92
Gruppeneigenschaften 119
Gruppenpriorität 121, 135
Gruppenressourcen 120
Gruppenzugriff
Konfigurationsbeispiele 318

H

Hardware
Installieren 41
Herunterfahren des Access Gateways 266
HOSTS-Datei 22
Bearbeiten 63
Hostüberprüfungsregeln, *siehe* Endpunktressourcen
HyperTerminal 44, 59
H.323-Protokoll 337

I

IAS, *siehe* Internetauthentifizierungsserver
ICA-Datei 208
ICA-Verbindung 209
ICA-Zugriffssteuerung 214
ICMP-Übertragungen 334
IEEE 802.11-Unterstützung 39
IETF, *siehe* Internet Engineering Taskforce
Inaktiver Server
Access Gateway Advanced Edition 38
Initialisieren des Access Gateways 266
Installation 45
Access Gateway 39
Administration Tool 45, 256
Administration Tool in Double-Hop-DMZ 232
Einzelne DMZ 25
Gerät in einer Double-Hop-DMZ 235
Hardware 41
Kreuzkabel 45
Lizenzen 51
Mehrere Stammzertifikate 61
Netzwerkkabel 45
Portalseiten 188
Secure Access Client 153
Secure Access Client für Linux 74
Stammzertifikate 60
Zertifikate 55, 58
Zertifikate, Administration Portal 59
Zubehör 39–40
Instant Messenging
AOL Instant Messenger 164
Gaim 158, 164
ICQ 164
IRC 164
MSN Messenger 164
Yahoo! Messenger 164

Internes Failover 170
Administration Tool 335
Internet Engineering Taskforce 292
Internetauthentifizierungsserver
RADIUS 96
Internet-Sicherheitsprotokolle 291
IP-Pooling 120, 168
ISO X.509-Protokoll 295

K

Kennwörter
Administrator 43, 258
Benutzer 85
Private Schlüssel für Zertifikate 57
Kennwortfelder 156
Kioskmodus 19, 120, 157
Aktivieren und Deaktivieren 159
Anmelden 190
Anwendungen 158
Clients 158
Dateien über FTP kopieren 166
Deaktivieren und Aktivieren 21
Firefox 158, 160
Freigegebene Netzlaufwerke 158
Freigegebene Netzlaufwerke verwenden 166
Gaim 164
Instant Messenging 164
Java Runtime Environment 334
Link zu Website 189
Persistenz 160
Remotedesktop 162
SSH-Client 163
Telnet 3270-Emulator-Client 163
VNC-Client 163
Zertifikat 334
Knowledge Center 15
Knowledge Center-Watches 16
Konfiguration
Anwendungsrichtlinie 129
Authentifizierung ohne Autorisierung 80
Benutzergruppen 117, 121
Endpunktressourcen 131
Endpunktrichtlinie 133
Lokale Benutzer 84
Netzwerkressource 126
Ressourcengruppen 119
Split-Tunneling 117
Standardgateway 46
Vorauthentifizierungsrichtlinien 137
Konfigurationsbeispiele
Anwendungsrichtlinie 322
Gruppenzugriff gewähren 318
LDAP-Authentifizierungsbereich 317
Lokale Autorisierung 329
Lokale Benutzer 325
Netzwerkzugriff 308
Zugängliche Netzwerke 315
Kreuzkabel 40, 45
Kryptografie 292–293
Allgemeine Informationen 291
Asymmetrische Verschlüsselung 293
Geheimschlüssel 293
Öffentlicher Schlüssel 293
Symmetrischer Schlüssel 293
Kulanzzeitraum
Lizenzen 54
Kurse 16

L

Lastausgleich 35
Double-Hop-DMZ 229
Laufwerkszuweisung
Zugriff einschränken 337
LDAP Browser 94
LDAP-Authentifizierung 28, 86, 142
Gruppenmitgliedschaft 91
Konfigurationsbeispiele 309, 317
Konfigurieren 88
Ports 86
Verzeichnisattribute suchen 94
Zertifikate 93
LDAP-Autorisierung 86, 90
Gruppenattribute 92
Konfigurationsbeispiele 309
Konfigurieren 92
Link Modes
Serielle Konsole 43
Linux-Unterstützung (Client) 74
Befehlszeilenoptionen 74
Client entfernen 74
Link zu Website 189
Neustart 74
Status überprüfen 74

Lizenzen
Abrufen 50
Aktualisieren 54
File does not match (Fehlermeldung) 333
Informationen 53
Installieren 49, 51
Kulanzzeitraum 54
Mehrere Geräte 52
Ports 53
Protokollierung 53
Testen 54
Lizenzierung 21
Firewall-Regeln 53
Lizenzserver 50
Load Balancer
Als Standardgateway festlegen 279
Geräte bereitstellen 275
Installations- und Konfigurationsprobleme 276
Lokale Authentifizierung 83, 142
Lokale Autorisierung
Konfigurationsbeispiele 329
Lokale Benutzer 117
Konfigurationsbeispiel 325
Konfigurieren 84
Mehrere Benutzergruppen 121
Lokale Benutzergruppen 119

M

MAC-Adresse
Benutzer deaktivieren und aktivieren 175
Maximum Transmission Unit 46
McAfee Personal Firewall Plus 268
Mehrere Anmeldeoptionen
Portalseite 190
Mehrere Ports 21
MTU, *siehe* Maximum Transmission Unit
Multi Router Traffic Grapher 286

N

Namensdienstanbieter 62, 339
Problembehandlung bei Namensauflösung 338
Namensscan 289
NetMeeting 337
Network Time Protocol (NTP) 70
Netzwerk
Flooding 336
Freigegebene Laufwerke 166
Paketdatenanalyse 289
Route-Tracing 289
Scannertools 289
Spamming 336
Split-Tunneling 116
Überwachen 288
Überwachung der Schnittstellenverkehrslast 290
Verbindungsfehler 336
Netzwerkadapter
Konfigurieren der TCP/IP-Einstellungen 45
Netzwerkaktivitätstimeout 120
Netzwerkgeschwindigkeit
Einstellen 46
Netzwerkinaktivitätstimeout 21, 171
Netzwerkkabel 40
Installation 45
Konfigurieren von TCP/IP 45
Netzwerkressource
CIDR nicht erkannt 334
Erstellen 126
Hinzufügen zu einer Gruppe 127
Netzwerkressourcen 18, 120
Zulassen und Verweigern 127
Netzwerkrouting 114
Netzwerkunterbrechung
Authentifizierung 167
Netzwerkzugriff
Citrix Presentation Server 214
Für Benutzer 114
Konfigurationsbeispiele 308
Konfigurieren 74
Routing 114
Neue Funktionen 20
Neustarten des Access Gateways 48, 265, 337
Node Secret 103
Norton Personal Firewall 269
NTLM-Authentifizierung 22, 28, 107, 142, 339
NTLM-Autorisierung 109
NTP, *siehe* Network Time Protocol (NTP)

O

Öffentliche Zertifizierungsstellen 299

P

Packliste 39
Paketdaten durchsuchen 289
Passthrough-Authentifizierung 216
Ping
  Befehl 334
  Serielle Konsole 43
  Von xNetTools 289
ping (Befehl) 42
PKI, *siehe* Public Key Infrastructure
Port
  Lizenzierung 53
  Scanner 289
Portalseite 120
  ActiveX-Steuerelement 152, 188
  Anpassen 187
  Benutzernamenvariablen 186
  Clientvariablen 186
  Installieren 188
  Konfigurieren 190
  Mehrere Anmeldeoptionen 190
  Standard 71
  Verbindung herstellen 72
  Vorlagen 185
  Vorlagen herunterladen 186, 258
  Zweimethodenauthentifizierung 191
Portbereiche 21
Ports
  Administration Portal 25
  Administration Tool 25
  Double-Hop-DMZ-Bereitstellung 234, 245
  Einzelne DMZ 25
  LDAP-Verbindungen 86
  Portbereiche 21
  Umleitung 47
Portumleitung 21, 47
Private Zertifizierungsstellen 299
Privater Schlüssel
  Entschlüsseln 302
  Installieren von einem Windows-Computer aus 60
  Kennwortgeschützt 57
  Kombinieren mit signiertem Zertifikat 304
Problembehandlung
  Webinterface 331
Produktdokumentation 15
Protokollierung 284
  Administration Portal 259
  Administration Tool 259
  Clientverbindungsprotokolle 285
  Lizenzen 53
  Serielle Konsole 43
Proxyserver
  Für Secure Access Client konfigurieren 148, 155
  Konfigurieren 148
Proxyservereinstellungen 21
Public Key Infrastructure 291

R

RADIUS-Authentifizierung 28, 95, 142
  Challenge/Response-Authentifizierung 22
  Internetauthentifizierungsserver konfigurieren 96
  Konfigurieren 97
  SafeWord PremierAccess 22
  SafeWord verwenden 105
RADIUS-Autorisierung 95
  Konfigurieren 98
RC4 20
Real-time Monitor 173, 289
  Gruppenprioritäten 137
Remotedesktop 158, 162
Ressourcen
  Dateifreigaben 120, 165
  Für Benutzergruppe konfigurieren 128
  Kiosk 120
Ressourcengruppen
  Entfernen von Benutzergruppen 128
  Konfigurieren 119
Richtlinien
  Anmeldeseiten 183
  IP-Pooling 168
RIP-Authentifizierung 65
Routen
  Dynamisches Routing konfigurieren 64, 66
  Statisch 67
  Statisches Routing konfigurieren 66–67
Routing
  Netzwerkzugriff 114
RSA ACE/Server
  Node Secret zurücksetzen 103
  sdconf.rec hochladen 102
RSA SecurID-Authentifizierung 28, 100, 142
  Cluster 103
  IP-Adresse einrichten 102
  Konfigurieren 102

S

SafeWord-Authentifizierung 22, 28, 104, 142
Konfiguration 105
Unterstützte Produkte 104
SafeWord-Autorisierung 106
Schulungen 16
sdconf.rec (Datei)
Cluster 103
Ersetzen 102
Hochladen 102
Ungültige Datei 336
Secure Access Client 18, 21
ActiveX-Steuerelement 152
Administratoren 149
Aktualisieren früherer Versionen 151
Anmelden 153, 190
Betrieb mit Proxyservern 148
Desktopfreigabe 21
Funktion zum automatischen Aktualisieren 338
Gleichzeitige Verbindung mit Citrix Presentation Server Clients 195
Installieren 153
IP-Pooling 168
Link zu Website 189
Linux-Unterstützung 74
Mit Firewalls verwenden 143
Mit Proxys verwenden 143
Proxyserver konfigurieren 148
Proxyservereinrichtung 155
Split DNS 169
Status 268
Systemanforderungen 140
Verbindung mit früheren Versionen 150
Verbindungsprotokoll 285
VPN-Software von Drittanbietern 339
Windows XP 338
Windows 2003 Server 338
Zugriffssteuerungsliste (Access Control List, ACL) 157
Secure Gateway
Ersetzen 197
Migrieren zum Access Gateway 201
Secure Socket Layer 142
Verschlüsselungsart auswählen 180
Secure Ticket Authority 28, 193
ICA-Datei 208
Sitzungsticket 208
Serielle Konsole 22
Administratorkennwort 43
Konfigurieren der TCP/IP-Einstellungen 42, 44
Optionen 43
Problembehandlung 336
Verwaltungsport aktivieren oder deaktivieren 43
Serielles Kabel 40
Serverfarm
Beschreibung 193
Serverzertifikat 295
Installation 300
Service 15
Sicherheit 27
Zertifikatverwaltung 27
Sicherheitskonzepte 291
Single Sign-On
Webinterface 216, 237
Windows 149
Sitzungsticket 208
ICA-Datei 208
Sitzungstimeout 21, 119–120, 171
Smartcard
Mit Webinterface 206
SNMP 286
Einstellungen 286
Gemeldete MIB-Gruppen 286
Protokolle aktivieren und anzeigen 286
Softphones 181
Speed Mode 46
Speicherbelegung 290
Speichern
Systemkonfiguration 264
Split DNS 120, 169
Split-Tunneling 116
Citrix Presentation Server 117
Konfigurieren 117
SSH-Client 158, 163
SSL (Secure Socket Layer) 291
SSL, *siehe* Secure Socket Layer
Stammzertifikate 179, 295
Erstellen über Eingabeaufforderung 62
Installieren 60, 179
Mehrere installieren 61
Standardgateway
Konfigurieren 46
Standardportalseite 71
Standardzertifikat
Zurücksetzen 59

Statische Routen
Beispiel 68
Entfernen 68
Hinzufügen 67
Testen 68
Statisches Routing 66–67
Testen 68
Statistiken 288
Status
Secure Access Client 268
Subscription Advantage 15
Sygate Personal Firewall 269
System Monitor 290
Systemanforderungen
Secure Access Client 140
Systemkonfiguration
Speichern 264
Wiederherstellen 264
Systemprotokoll
Anzeigen 283
Archiv 283
Downloaden 283
Filtern 283–284
Weiterleiten an Systemprotokollserver 286
Systemprotokollserver, Weiterleiten des Systemprotokolls 286
Systemstatistiken 288

T

TCP/IP-Einstellungen
Double-Hop-DMZ 48
Konfigurieren mit Netzwerkkabeln 45
Konfigurieren mit seriellem Kabel 44
Serielle Konsole 42
Technischer Support 15
Telnet 3270-Emulator-Client 158, 163
Testzertifikate 300
Ticketing 208
ICA-Datei 208
Timeout 21
Benutzersitzung 119, 171
Inaktive Sitzung 120, 171
Netzwerkinaktivität 120, 171
Websitzung 172
Timeout wegen inaktiver Sitzung 120, 171
Tiny Personal Firewall 269
TLS (Transport Layer Security) 291
TLS, *siehe* Transport Layer Security
Traceroute-Tool 289
Transport Layer Security 142

U

Über Access Gateway zugängliche Netzwerke
Secure Access Client-Fenster 157
Überprüfungsintervall
Access Gateway Advanced Edition 38
Überwachungstool 288
Uhrzeit
Einstellungen 70
Synchronisieren
Umleitung
Ports 21, 47
Unsichere Verbindungen
Umleiten 47
Unterstützung 15–16

V

Verbindungen
Access Gateway Advanced Edition 19
Citrix Presentation Server 194
Citrix Presentation Server Clients 195
Client kann keine Verbindung herstellen 336
Deaktivieren 173
Double-Hop-DMZ 225
Einzelne DMZ 25
Gleichzeitig 18
Hardware 41
ICA 209
Kioskmodus 19
LDAP-Zertifikate 93
Mit Secure Access Client und Citrix Presentation Server Clients 195
Nur über Access Gateway 18
Schließen 173, 175
Serverfarm 30
Unsichere Verbindungen umleiten 21
Verarbeiten 174
Webadresse verwenden 152
Webinterface 18
Verbindungsprotokoll
Secure Access Client 285
Verschlüsselung 20
Asymmetrisch 293
Öffentlicher Schlüssel 294
Verschlüsselungssammlungen auswählen 180
Verschlüsselung mit öffentlichem Schlüssel 294
Verschlüsselungssammlungen 20
Beschreibung 292
Verweigern des Zugriffs ohne Zugriffssteuerungsliste 115, 118

Verzeichnisattribute
LDAP 94
VMWare 333
VNC-Client 158, 163
VoIP (Voice over IP) 22, 181
Latenz verbessern 182
Vorauthentifizierungsrichtlinien
Anmelden 192
Konfigurieren 137
Vorlagen
Portalseite 185, 258
Portalseite anpassen 187
Vom Administration Portal 258
Von Portalseite herunterladen 186

W

Wartung
Administration Portal 259
Administration Tool 256
Webadresse des Administration Portals 260
Webbrowser
Firefox 158
Webinterface 18, 120
Als Anmeldeseite konfigurieren 216
Anmelden 190
Anwendungen nicht verfügbar 331
Authentifizierung 193, 207
Bereitstellen im sicheren Netzwerk 207
Bereitstellen mit dem Access Gateway 204
Bereitstellen parallel zum Access Gateway 205
Bereitstellung 28
Bereitstellung im sicheren Netzwerk 30
Bereitstellung in DMZ hinter Access Gateway 30
Bereitstellung in DMZ parallel zum Access Gateway 30
Hinter Access Gateway bereitstellen 206
ICA-Zugriffssteuerung 214
Problembehandlung 331
Single Sign-On 216, 237
Smartcard-Bereitstellung 206
Zugriff ohne Anmeldeinformationen 331
Websitzungstimeout 172
whois-Abfrage 289
Wiederherstellen der Systemkonfiguration 264
Windows
Anmeldeskripte 170
Single Sign-On 149
Windows NT LAN Manager, *siehe* NTLM-Authentifizierung
Windows XP
Secure Access Client 338
WINS
Problembehandlung 339
WINS-Server
Einstellungen 62
Secure Access Client-Fenster 157

X

xNetTools 289
X.509-Standard 296

Z

Zertifikate 27, 291, 295
Ablaufen 298
Access Gateway Advanced Edition 178
Authentifizierung 295
Client 120, 176–177
Double-Hop-DMZ-Bereitstellung 234
Einstellungen 58
Erneuern 298
Für mehrere Ebenen generieren 304
Hierarchie 296
In PEM-Format umwandeln 302
Inhalt 296
Installation 55, 300
Installieren mit Administration Portal 59
Installieren mit Administration Tool 58
Installieren von einem Windows-Computer aus 60
Kennwort für privaten Schlüssel 57
Ketten 296
Kombinieren mit privatem Schlüssel 304
LDAP-Verbindungen 93
Mehrere Ebenen und SSL Version 2 337
Mehrere Stammzertifikate 61
Mehrere Stammzertifikate über Eingabeaufforderung erstellen 62
Privat 299
Privaten Schlüssel entschlüsseln 302
Serverzertifikat 295
Signieren 335
Sperrlisten 298
Stammzertifikat 295
Stammzertifikate 60, 179
Stammzertifikate unter Windows installieren 179
Testzeitraum 300
Testzertifikat 300
Untergeordnete Zertifizierungsstellen 297
Verifizierungsprozess 299
Wiederherstellen des Standardzertifikats mit der seriellen Konsole 43
Zertifikatketten 296
Zertifikatsignieranforderung 56
Zurücksetzen auf Standardzertifikat 59
Zwischenzertifizierungsstellen 297
512-Bit-Schlüsselpaare 337
Zertifikatketten 296
Zertifikatsignieranforderung
Erstellen 57
Übersicht 56
Zertifikatsperrlisten 298, 335
Zertifizierungsstelle
Stammzertifikat abrufen 179
Zertifizierungsstellen 295–296
Öffentlich 299
Privat 299
Untergeordnete Zertifizierungsstellen 296
ZoneAlarm Pro 270
Zubehör
Access Gateway-Installation 40
Double-Hop-DMZ-Bereitstellung 234
Zugängliche Netzwerke 116
Einschränkungen 333
Konfigurationsbeispiele 315
Zugriffssteuerungsliste (Access Control List, ACL) 123
ICA-Zugriffssteuerung 214
Regeln zum Zulassen und Verweigern 128
Secure Access Client-Eigenschaften 157
Zugriff ohne ACL verweigern 115
Zugriff verweigern 118
Zweimethodenauthentifizierung 110, 191
3DES 20